



2022  
SONICWALL  
CYBER  
THREAT  
REPORT

---

SONICWALL®

CYBER THREAT INTELLIGENCE FOR NAVIGATING  
THE UNKNOWN OF TOMORROW

[sonicwall.com](https://sonicwall.com) | [@sonicwall](https://twitter.com/sonicwall)



# Table of Contents

---

<b>Introduction</b>	<b>3</b>	<b>Cryptojacking</b>	<b>40</b>
A Note From Bill	3	Bigger than Ever	40
2022 Global Cyberattack Trends	4	Cryptojacking by Region	41
2021: A Turning Point in the War on Ransomware	5	Cryptojacking by Industry	42
<b>Supply Chain</b>	<b>8</b>	<b>Encrypted Attacks</b>	<b>45</b>
Supply-Chain Attacks Continue In 2021	8	Encrypted Attacks Show Triple-Digit Increase	45
<b>CVEs</b>	<b>9</b>	<b>Intrusion Attempts</b>	<b>47</b>
Published CVEs Break 20,000 for the First Time	9	Malicious Intrusion Attempts Fall By Nearly a Third	47
2021 Zero-Day Vulnerabilities	11	<b>Capture ATP &amp; RTDMI</b>	<b>51</b>
The Log4j Vulnerability	12	RTDMI Gets Smarter, Faster, Better	51
<b>Business Email Compromise</b>	<b>15</b>	<b>Malicious PDF/Office Files</b>	<b>53</b>
The Impersonators in Your Inbox	15	Malicious Office and PDF Files Reverse Course	53
<b>Key Findings from 2021</b>	<b>17</b>	<b>IoT Malware</b>	<b>57</b>
<b>Malware</b>	<b>19</b>	IoT Malware Shows Signs of Stabilizing	57
Malware May Be Headed for a Rebound	19	IoT Malware by Industry	59
Malware by Region	20	<b>Attacks on Non-Standard Ports</b>	<b>62</b>
Malware Spread by Country	21	Non-Standard Port Attacks Fall 10%	62
Malware Risk by Country	23	<b>Conclusion</b>	<b>64</b>
Malware by Industry	28	Proactive Defense is the Future of Cybersecurity	64
<b>Ransomware</b>	<b>29</b>	About the SonicWall Capture Labs Threat Network	65
Ransomware's Savage Reign	29		
Ransomware by Region	31		
Top Ransomware by Signature	33		
2021 Ransomware Trends	37		

# Introduction

## A Note From Bill



As the world continued to grapple with the challenges of 2020, such as the ongoing COVID-19 pandemic, 2021 brought its own set of new challenges. Supply-chain woes in 2021 affected everything from healthcare, the automotive industry and cybersecurity to travel, retail and the food supply.

The growing pains of the new work reality were evident as companies opting for a permanent shift to fully remote work often found their networks, employees and processes unprepared for the change. Many businesses that stayed with the traditional work model continued to make arrangements for employees to return to the office, only to find time and again that the pandemic had other plans.

Cybersecurity faced its own set of increased challenges in 2021. The year was bookended by two major incidents: the SolarWinds attack in December 2020 and the Log4j vulnerabilities in 2021. In between, ransomware rose dramatically, far surpassing the levels we found alarming in 2020. Most other attack types showed increases as well, including overall malware, which had been on a downward slide for years.

But while some may see these challenges and default to pessimism, doing so requires an impossibly narrow view of the preceding year — one which doesn't stand up to scrutiny.

When I look back on 2021, I'm amazed at what was accomplished. SonicWall made key engineering and manufacturing changes, ensuring our partners and end users were largely unimpacted by supply-chain disruptions. We also completed the Gen 7 refresh of our next-generation firewalls, making our platform stronger, easier to use and more reliable, and unifying our portfolio across hardware, software and cloud.

Businesses outside of cybersecurity also doubled their efforts to fight cybercrime. From mid-2020 to 2021, the number of CEOs who said cybersecurity risks were the biggest threat to short-term growth [nearly doubled](#), and corporate boards are increasingly [forming cybersecurity committees](#).

This has translated to increased funding: Global cybersecurity spending [was projected to grow](#) 12.4% by the end of 2021, twice as fast as in 2020.

At the government level, at least 45 U.S. states [considered cybersecurity bills in 2021](#), up 18% from 2020. And the [U.S.](#), [Japan](#), [Australia](#), [Germany](#) and countless others passed measures [strengthening national cybersecurity](#).

But perhaps most remarkable is the level of cooperation 2021 brought. Governments are increasingly [coordinating with business and education leaders](#) on "whole-of-nation" efforts.

In June, the Group of Seven (G7) [called for](#) greater accountability in countries harboring ransomware groups. And in October, leaders from 30 countries [met to formulate an international response](#) to cybercrime. Few enemies, in our time or any other, have prompted such a unified effort.

There will be years that test us — and 2021 certainly did that — but it didn't find us wanting. Instead, it found us, as a company, as an industry, as a *civilization* — innovating, fortifying, unifying. And while cybercriminals may have notched some battles this past year, in the end they spurred us on. If they want to win, they'll have to take on all of us, together.

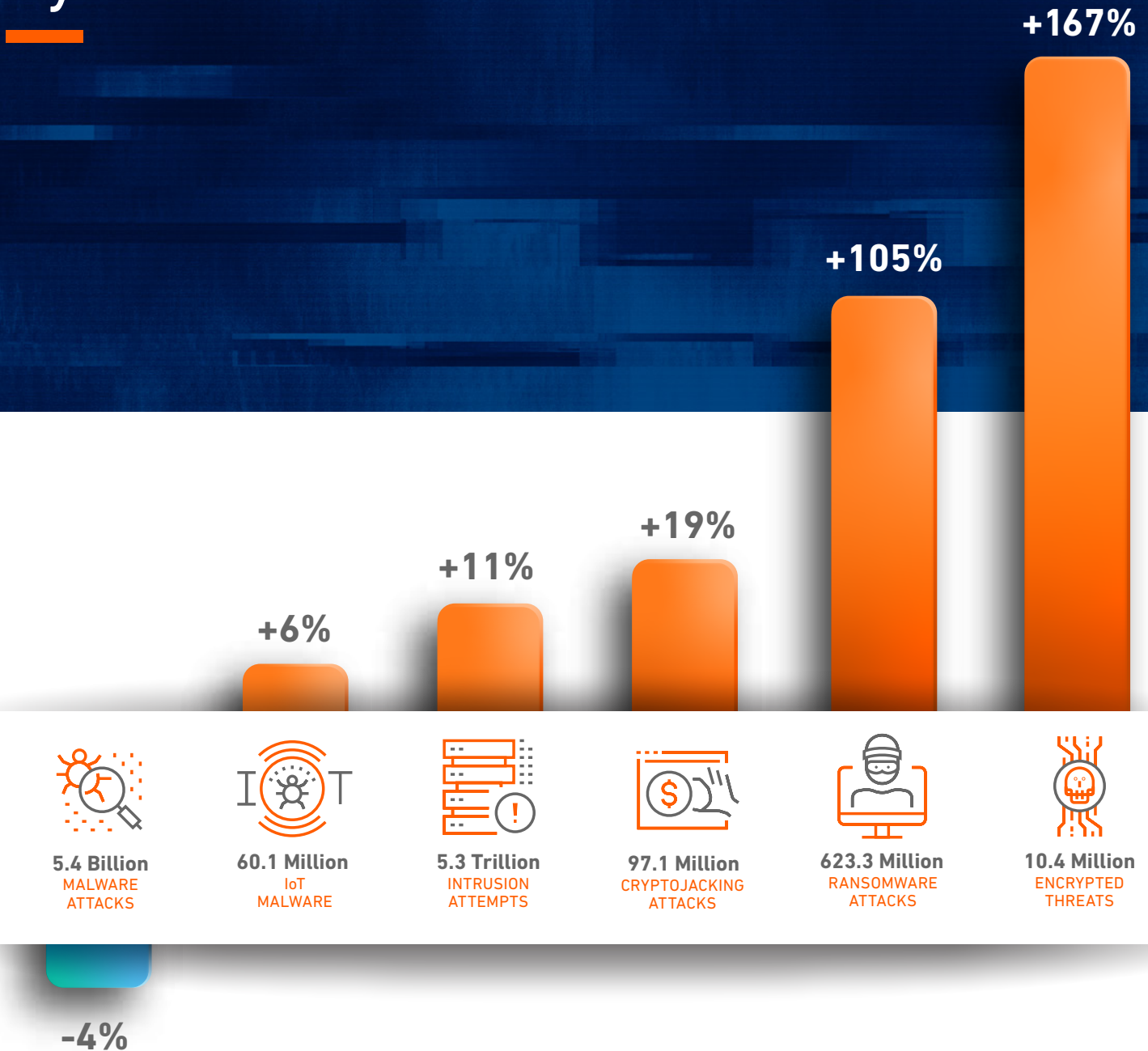
In this spirit of cooperation, we're pleased to share with you the 2022 SonicWall Cyber Threat Report — full of research on cybercriminal behavior, industry trends and insight on what 2022 might have in store.

A stylized, handwritten signature in black ink that reads "Bill Conner". The signature is fluid and cursive, with the first letters of the first and last names being significantly larger and more prominent.

**BILL CONNER**  
PRESIDENT & CEO  
SONICWALL



# 2022 Global Cyberattack Trends



As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.



# 2021: A Turning Point in the War on Ransomware

Five years ago, a debate erupted surrounding the infamous NotPetya cyberattack: Did it constitute an act of war?

This issue [continued to be debated](#) in the courts throughout 2021, but on the battlefields of business networks around the world, cybercriminals were launching a full-bore offensive.

Ransomware climbed an unprecedented 105% in 2021, and the explosive growth of strategies such as [double](#) and even [triple extortion](#) ensured that these attacks were more successful than ever. But as cybercriminals have grown more sophisticated and successful, they've also grown more ruthless — many of the high-profile ransomware attacks in 2021 looked more like acts of war than ever before, endangering our [food supply](#), our [water supply](#), our [fuel supply](#), our [hospitals](#) and our [municipalities](#).

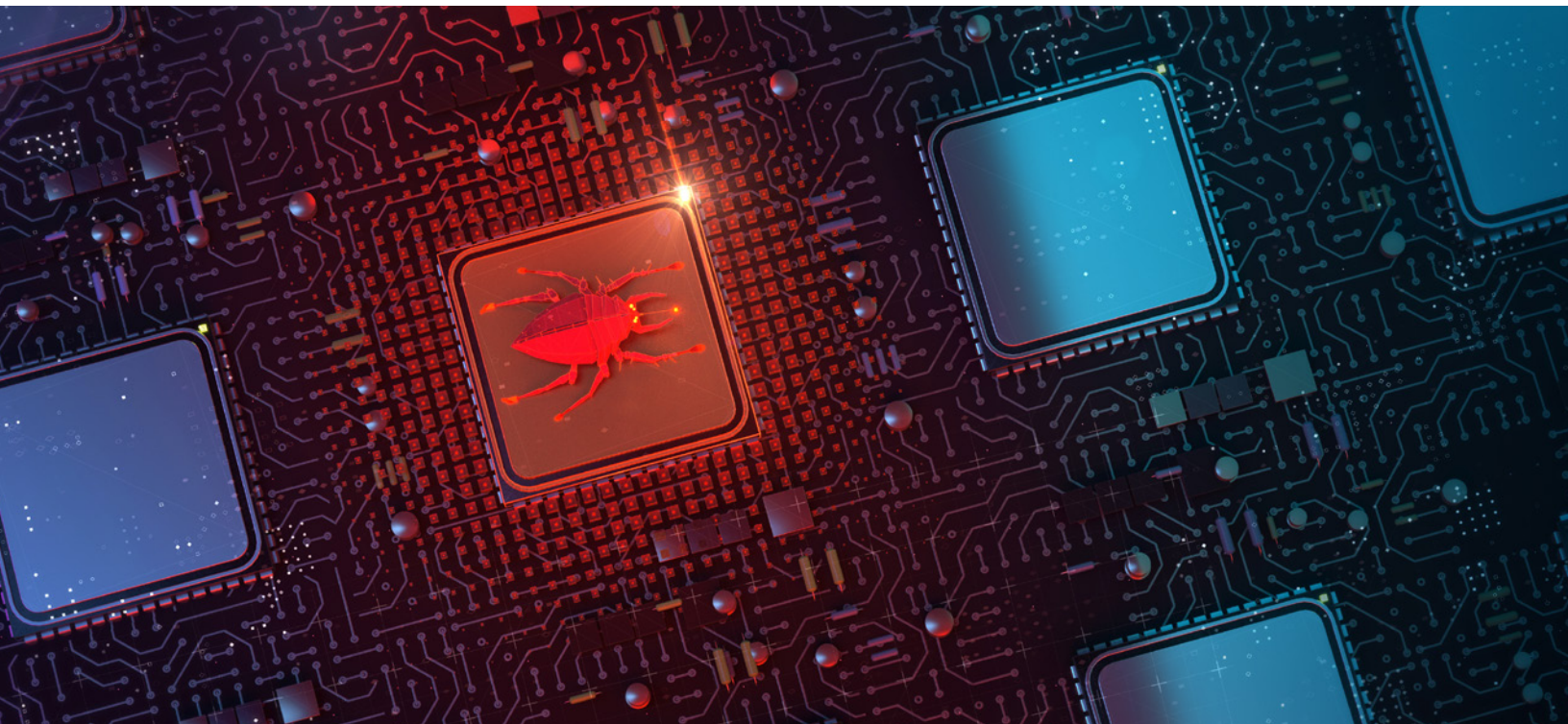
That the courts ultimately decided cyberattacks such as NotPetya [do not, in fact, constitute acts of war](#) is irrelevant: Fed up with cybercriminals growing rich off their constituents, leaders around the world — from the [local level](#) to the [international stage](#) — have brought the war to them.


The UN Cybersecurity Open-Ended Working Group in March 2021 [endorsed a report](#) containing cybersecurity recommendations, the first time that a process open to all countries has resulted in consensus on international cybersecurity.

In May 2021, U.S. President Joe Biden issued a [sweeping executive order](#) on cybersecurity, which unifies cybersecurity standards across government agencies, emphasizes zero-trust principles and provides specific timelines for action.

In July, [INTERPOL held its forum on ransomware](#). Advising that effectively preventing and disrupting ransomware would require “adopting the same international collaboration used to fight terrorism, human trafficking or mafia groups,” the group called for police agencies worldwide to form a global coalition with industry partners to stop ransomware’s exponential growth.

But perhaps the biggest testament to the threat ransomware poses to national security is the involvement of the U.S.





military. In an interview with [The New York Times](#), U.S. Cyber Command head Gen. Paul M. Nakasone explained that, while he once saw ransomware as the responsibility of law enforcement, attacks such as Colonial Pipeline and JBS represented a big enough threat to the nation's critical infrastructure to warrant a more aggressive approach.

But this approach likely won't include boots on the ground — an option that proves challenging given that a vast majority of these ransomware operators are in other countries, most of which are not U.S. allies and tend to only go after cybercriminals when it [serves their agenda](#).

While high-profile arrests of cybercriminals continue, such as the [REvil takedown in early 2022](#), they have been largely ineffective in stemming the tide of ransomware itself. The amount of time and resources required for each bust means that the criminal justice system is [unable to keep up](#) with the huge number of ransomware operators. And due to the lucrative nature of ransomware, as soon as one group is taken down, new ones rise to fill the void.

Instead, this approach will look a lot like their most ruthless attacks on civilians: a direct assault on their infrastructure. Pressure on the U.S. government to deploy intelligence and military solutions to attack the servers, networks and more used for cybercrime, dissemination of stolen data on the dark web and storing cryptocurrency payments is growing.

While he refrained from giving details, Nakasone confirmed that [the military has taken an offensive stance](#) against ransomware groups. One known example is when Cyber Command assisted in the [recovery of millions in ransom](#) that Colonial Pipeline paid to attackers.

Though recoveries such as this have historically been rare, this may be the first in an emerging trend. A major factor credited in this recovery is the work of a recently formed [Ransomware and Digital Extortion Task Force](#). In an interview with [Reuters](#), a senior U.S. DOJ official said the formation of this task force “elevates investigations of ransomware attacks to a similar priority as terrorism.”

As the amount of media attention and government involvement in the wake of high-profile attacks increases, these groups have grown wary, with many [laying low](#) or [disappearing altogether](#). This could lead to groups lowering ransom demands in hopes of flying under the radar and continuing to hack another day — which could contribute to fewer attacks if success no longer means netting a life-changing fortune for the entire syndicate.

In other words, in the end, the most lethal shots to ransomware may well be the ones that hit where it hurts most: the wallet.

## Cybersecurity is Infrastructure

On Nov. 15, U.S. Pres. Joe Biden signed into law the Infrastructure Investment and Jobs Act. While the bulk of the \$1.2 trillion investment targets the country's crumbling bridges, tunnels, roads and railways, it also provides \$2 billion for cybersecurity, reaffirming the role of cybersecurity as part of the country's 21st century infrastructure.

About half of that amount is set aside for the State, Local, Tribal and Territorial (SLTT) Cyber Grant Program and will be distributed over four years. The Act's language offers much-needed guidance on the types of investments that governments are expected to make — specifically, firewalls

(on-prem and virtual), secure mobile access (on-prem and virtual) and advanced software that provides endpoint threat detection and response.

The legislation also earmarks \$42.45 billion for the “Broadband Equity, Access, and Deployment” initiative, which will expand grants available to underserved communities. This funding is expected to touch on local cybersecurity considerations as expansion will likely involve wireless communication and participation from local utilities (e.g., mobile, broadband).

## Beyond Ransomware: The Threat of BEC, Phishing and More

While ransomware attracted most of the headlines in 2021, the year's data pointed to plenty of other areas of concern.

Based on data collected by SonicWall Capture Labs threat researchers, while ransomware did make up the largest number of malware signatures detected, it amounted to only about a quarter of the total volume.

According to a recent report from Gartner, the percentage of respondents rating vulnerabilities as "very important" is higher than the percentage who assigned this rating to ransomware. Fortunately, increased awareness may translate to fewer successful attacks, as Ponemon Institute recently reported that unpatched vulnerabilities were a factor in [more than half of all data breaches](#), and over 60% of those surveyed said they were unaware of vulnerabilities in their organization before they were breached.

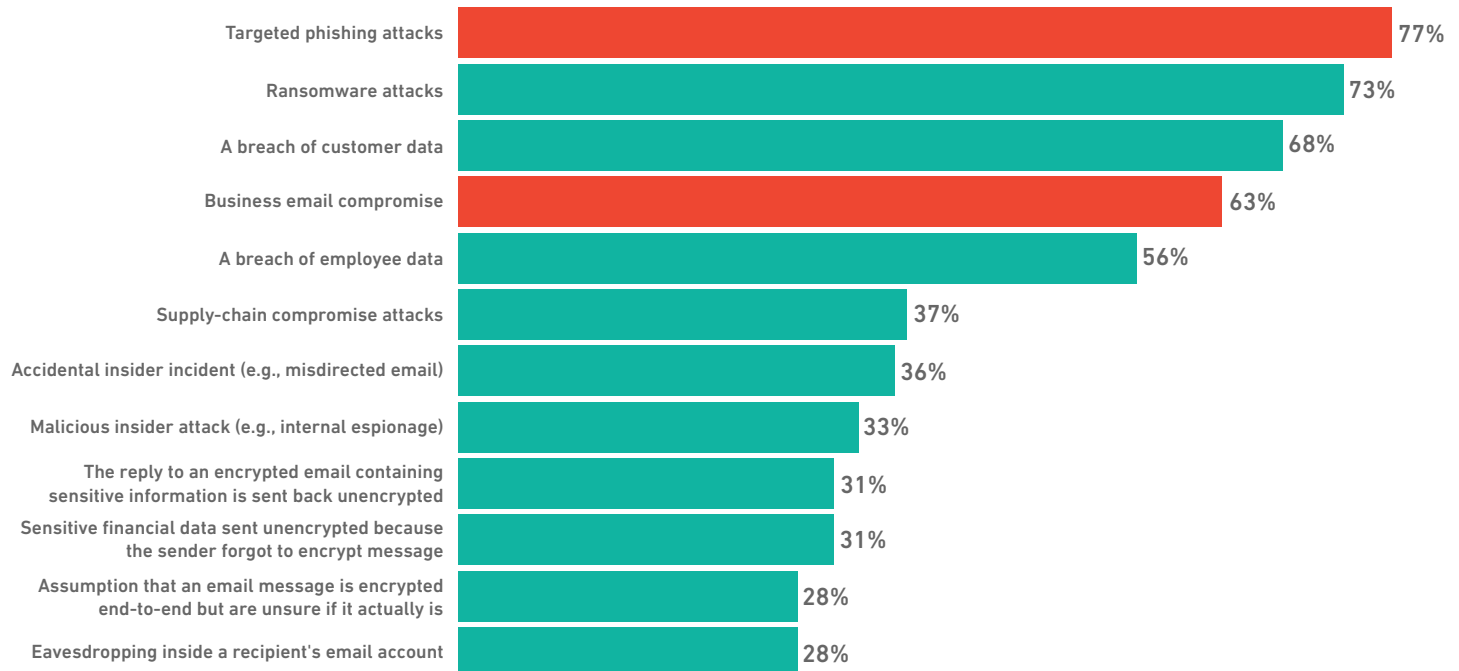
A recent [SonicWall-sponsored survey by Osterman Research](#) painted a slightly different picture. This group of respondents ranked phishing attacks as their top concern (though, again, ransomware was a close second.)

Nearly 2/3 of respondents also rated Business Email Compromise (BEC) attacks as an area of concern. While these attacks may not get the headlines that ransomware attacks do, according to the Internet Crime Complaint Center (IC3), BEC attacks are the costliest, with 19,369 reports and a total loss of \$1.8 billion [in 2020 alone](#).

Due to the dangers posed by infrastructure attacks and leaks of sensitive data, ransomware may continue to be the focus of governments and law enforcement in the short term. But these trends are a good sign that as other attack types continue to grow and rise in severity, organizations are keeping an eye on the bigger picture.

### Level of Concern About Types of Cyberattacks

Percentage of respondents indicating "concerned" or "extremely concerned"



\*How to Deal with Business Email Compromise,\* Osterman Research, Sponsored by SonicWall, January 2022



# Supply Chain

## Supply-Chain Attacks Continue In 2021

In December 2020, American company SolarWinds confirmed that a version of its Orion product had been targeted via the company's supply chain, kicking off a new era in supply-chain attacks.

These attacks, referred to as "supply-chain attacks" because they infiltrate the products or services of a trusted business partner instead of targeting a company directly, are by no means new: They date back to at least 2013, when American retailer Target [was attacked via its HVAC supplier](#). But it wasn't until [NotPetya's spread in 2017](#) that people really started to understand the widespread devastation that supply-chain attacks could wreak.

Five years later, a new crop of supply-chain attacks made their mark across 2021 — many not just threatening profits and business continuity, but striking directly at our daily lives. Here are some of the year's worst:

### Accellion – Dec. 2020-Jan. 2021

A total of four major vulnerabilities were identified in American technology company Accellion's FTA server, a file-transfer program. The first two, exploited in December 2020, were quickly patched — but unbeknownst to Accellion at the time, [two additional CVEs](#) were being exploited through January. The attack spread to as many as 100 of Accellion's customers via the impacted FTA server. The hackers stole large quantities of sensitive personal information, which the CIOp ransomware gang used to extort payment from the victims.

Perhaps as remarkable as the breach itself is the fact that it didn't happen sooner: The FTA server in question was a 20-year-old legacy product that [advertised itself as a way to securely transfer sensitive files](#), and the fact that it has long been utilized by major players in governments, the insurance industry and the financial sector means it's likely been an attractive target for a long time.

### Codecov – April 15, 2021

In April, software company Codecov became aware that attackers had compromised an uploader designed to deliver coverage data and product updates. This attack went undetected for [more than two months](#), allowing the attackers to steal credentials and exfiltrate sensitive data from an unknown number of the company's 29,000 clients — a list which included [Proctor & Gamble](#), [Atlassian](#), [GoDaddy](#), [The Washington Post](#) and [IBM](#).

### Kaseya – July 2, 2021

Just before the U.S. July 4 holiday, a massive ransomware campaign then called the "[single biggest ransomware attack yet](#)" came to light. By gaining access to American software company Kaseya's [VSA remote management and monitoring software](#), ransomware group REvil was able to impact Managed Service Providers (MSPs), and in turn, gain access to their clients. An estimated [1,500 organizations](#) in at least [17 countries](#) were affected.

### Python Package Index (PyPI) – July 29, 2021

In July, 11 Python packages hosted on open-source repository PyPI, the official third-party software repository for Python, were found to contain malicious code. Due to the fact that the malware packages were remarkably well hidden, the packages remained undetected for long enough to be [downloaded over 41,000 times](#) by developers from other organizations. These [malicious files](#) then stole Discord authentication tokens, scraped sensitive autocomplete data, and mined system information including IP address, user name, license key information and more.

# CVEs

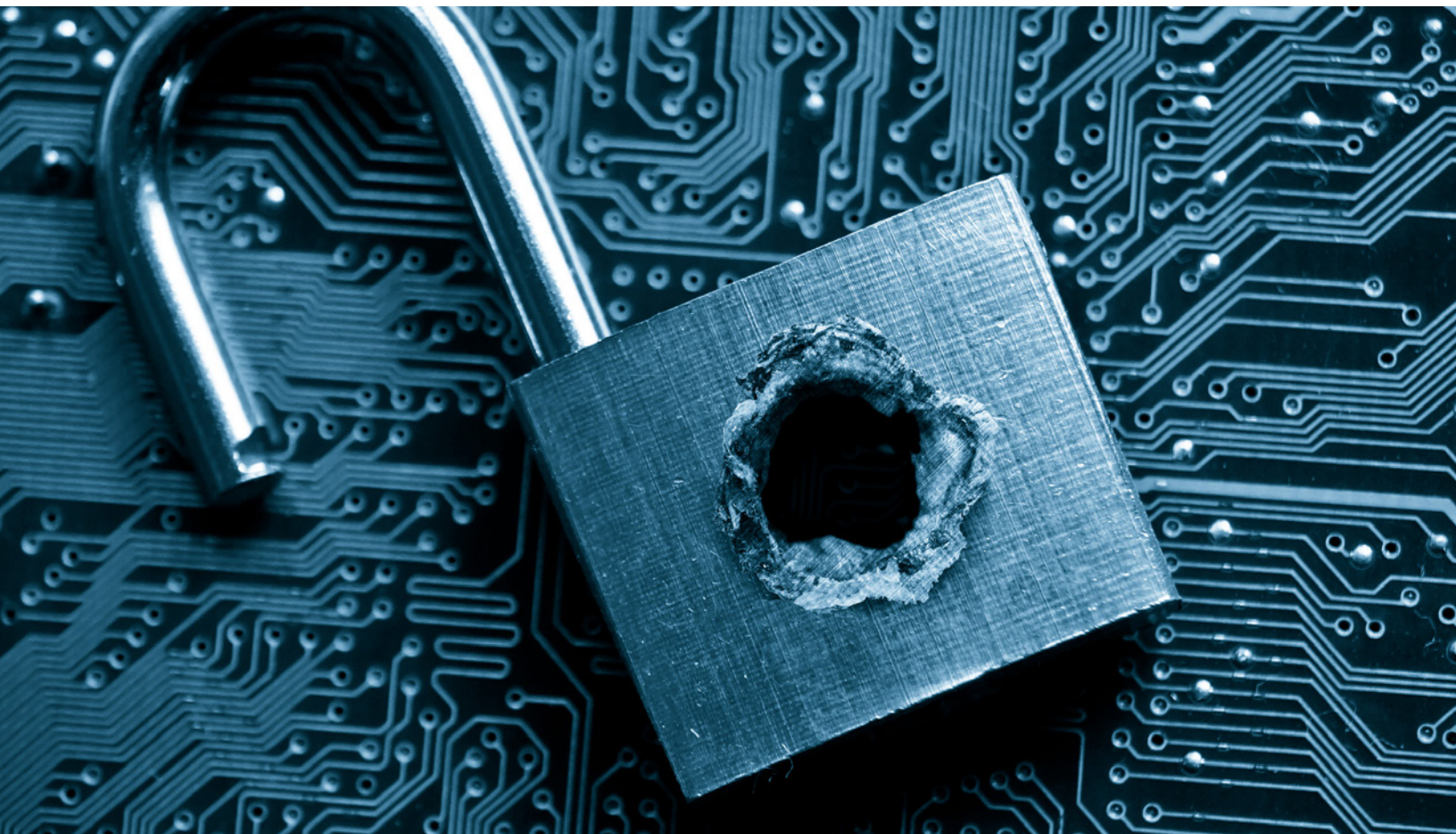
## Published CVEs Break 20,000 for the First Time

According to NIST, 20,136 Common Vulnerabilities and Exposures (CVEs) were published in 2021. This marks the fifth year in a row that a record number of vulnerabilities has been discovered, and the first time in history that the number of CVEs has passed the 20,000 mark.

This isn't necessarily a milestone to celebrate, however. While the number of vulnerabilities reflects the hard work those in the cybersecurity industry are doing to identify vulnerabilities more quickly and efficiently, it also reflects pernicious trends that make quicker and more efficient work necessary in the first place.

One is the growing attack surface resulting from organizations deploying more software and tools as they continue their digital transformation. The more products a company utilizes, the more likely one of them will be vulnerable.

The most serious of these vulnerabilities, those scored above nine on the 10-point scale, become entry points for cybercriminals, and attackers are increasingly utilizing this means of entry to deploy ransomware and steal data.



## History Repeating: 80% of Top 10 Exploited Vulnerabilities Are From Previous Years

In July 2021, CISA released its [list of top vulnerabilities exploited by cybercriminals](#) in 2020. Each of the top ten most exploited vulnerabilities has a patch or an updated version available for devices — yet out of the top 10 vulnerabilities exploited in 2020, only two were *actually discovered* in 2020.

The number of entirely preventable exploits once again highlights the need for more timely and widespread patching.

In addition, SonicWall identified a number of even older vulnerabilities being actively exploited, including CVE-2013-3541, CVE-2016-1605, CVE-2014-6036 and many more.

## Top 10 Most Exploited Vulnerabilities

CVE	VENDOR/PROJECT	PRODUCT	TYPE
CVE-2019-19781	Citrix	Citrix ADC and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0	Arbitrary Code Execution
CVE 2019-11510	Pulse	Pulse Secure Connect VPN 8.2, 8.3 and 9.0	Arbitrary File Reading
CVE 2018-13379	Fortinet	Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7, and 5.4.6 to 5.4.12	Path Traversal
CVE 2020-5902	F5- Big IP	BIG-IP 15.1.0, 15.0.0-15.0.1, 14.1.0-14.1.2, 13.1.0-13.1.3, 12.1.0-12.1.5, and 11.6.1-11.6.5	Remote Code Execution (RCE)
CVE 2020-15505	MobileIron	MobileIron Core & Connector 10.3.0.3 and earlier, 10.4.0.0 to 10.4.0.3, 10.5.1.0, 10.5.2.0, and 10.6.0.0; Sentry 9.7.2 and earlier and 9.8.0; and Monitor and Reporting Database (RDB) 2.0.0.1 and earlier	Remote Code Execution (RCE)
CVE-2017-11882	Microsoft	Microsoft Exchange Server 2019 Cumulative Update 3 and 4, 2016 Cumulative Update 14 and 15, 2013 Cumulative Update 23, and 2010 Service Pack 3 Update Rollup 30	Remote Code Execution (RCE)
CVE-2019-11580	Atlassian	Crowd version 2.1.0 before 3.0.5, version 3.1.0 before 3.1.6, version 3.2.0 before 3.2.8, version 3.3.0 before 3.3.5, and version 3.4.0 before 3.4.4	Remote Code Execution (RCE)
CVE-2018-7600	Drupal	Drupal versions before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1	Remote Code Execution (RCE)
CVE 2019-18935	Telerik	Telerik UI for ASP.NET AJAX versions prior to R1 2020 (2020.1.114)	Remote Code Execution (RCE)
CVE-2019-0604	Microsoft	Microsoft Sharepoint 2019, Microsoft SharePoint 2016, Microsoft SharePoint 2013 SP1, and Microsoft SharePoint 2010 SP2	Remote Code Execution (RCE)

CISA, Top Routinely Exploited Vulnerabilities, 2021



# 2021 Zero-Day Vulnerabilities

Of the more than 20,000 new CVEs published in 2021, 14 were published immediately to identify and correct zero-day vulnerabilities.

Month	CVE	Vulnerability
January	CVE-2021-1782	Elevation of privilege vulnerability in Apple
February	CVE-2021-21148	Heap buffer overflow in V8 in Google Chrome
March	CVE-2021-26855	Microsoft Exchange server remote code execution vulnerability [Hafnium]
March	CVE-2021-26857 CVE-2021-26858 CVE-2021-27065	Microsoft Exchange server remote code execution vulnerability [Hafnium]
March	CVE-2021-24175	Authentication bypass in Elementor Page Builder WordPress plugin
March	CVE-2021-21193	Use after free in Blink in Google Chrome
May	CVE-2021-22893	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability
May	CVE-2021-28550	Use after free vulnerability in Acrobat Reader DC
May	CVE-2021-30713	Arbitrary code execution in Apple MacOS
July	CVE-2021-30116	Kaseya VSA credential disclosure [REvil ransomware]
August	CVE-2021-36958	Windows Print Spooler remote code execution vulnerability
December	CVE-2021-44228	Remote code execution vulnerability in Apache Log4j



# The Log4j Vulnerability

While the Apache Log4j vulnerability was the final major vulnerability identified in 2021, it quickly became one of the most exploited. From Dec. 11 to Jan. 31, SonicWall recorded 142.4 million exploit attempts against Log4j vulnerabilities — an average of 2.7 million each day.

What’s remarkable, though, is how quickly hackers and cyber threat actors pivoted to exploit these vulnerabilities. It took less than 48 hours from the initial Dec. 9 PoC public disclosure for attempted exploits to reach into the hundreds of thousands, and by the third day attempts had already passed the 1 million mark.

Since then, the Log4j vulnerabilities have been exploited across all industries. But the hardest hit so far have been the scientific and technical community (28%), manufacturing (13%), government (9%), finance (5%), retail (5%) and K-12 (5%).

To date, SonicWall has released eleven signatures to help safeguard our customers against the widespread exploitation of the Log4j vulnerabilities.

## What are the Log4j Vulnerabilities?

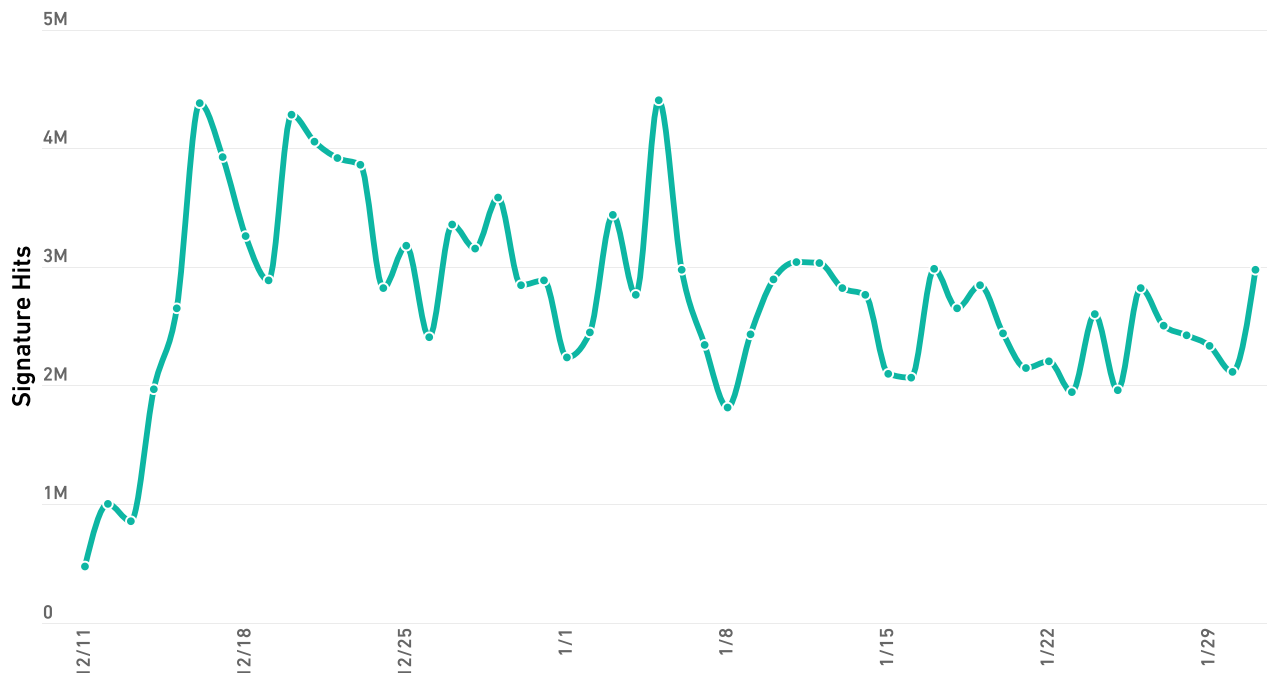
The vulnerabilities affect Log4j, an extremely popular Full Open-Source Software (FOSS) logging library with two primary branches: 1.x and 2.x, the former of which is at end-of-life. The primary vulnerabilities are tracked via [CVE-2021-44228](#), [CVE-2021-45046](#) and [CVE-2021-45105](#).

Based on [Google’s Open Source Insight Team’s examination](#), Log4j was identified as a ubiquitous dependency across 35,000 packages — or 10% of all packages — and is bundled with the widely adopted Apache Server.

The first and most critical vulnerability among the suite, CVE-2021-44228, was initially referred to as “Log4shell,” a name now commonly used to describe the entire suite of vulnerabilities. As scrutiny of Log4j continues by both the cybersecurity industry and attackers, a continuous stream of additional vulnerabilities is expected to be identified for the foreseeable future.

While keeping up the cadence of patches for these vulnerabilities will pose a challenge, the real struggle will be in identifying impacted frontends, middleware, backends, desktop apps, off-the-shelf software and software created in house.

### Malicious Log4J Exploit Attempts



## Who's Affected?

The rate of exploit makes it difficult for patch development to keep up. But even when it can, it isn't a panacea: Patching hygiene is enough of a challenge in perfect conditions. But because this vulnerability affects millions of consumer and business products — everything [from the Minecraft video game to the Mars 2020 helicopter mission Ingenuity](#) — getting everyone to care enough to patch even once is an uphill battle, to put it mildly.

Even so, it wouldn't be enough. Stores and warehouses are full of products packaged with Log4j that will become vulnerable the minute they come online, and some legacy products are no longer receiving updates at all, including [some critical healthcare systems](#).

## What are the Dangers?

Because this vulnerability is due to improper handling of logged messages, any remote, unauthenticated attacker who can control log message contents can exploit the vulnerability. This can be done by sending a specially crafted parameter to the target application. From there, attackers can break into systems, steal passwords and logins, extract data and infect networks with malicious software.

## The Conti Connection

It took less than a week for this exploitation to start happening. As early as Dec. 13, the Conti ransomware group exploited the Log4Shell vulnerability to [access VMware vCenter servers](#), then moved laterally within the corporate network.

## Log4Shell Timeline

- 11.24.2021**
  - Vulnerability disclosed by Alibaba to Apache
  - Logged in Log4j2-3198
- 12.09.2021**
  - PoC is publicly disclosed resulting in initial scans and exploitation
- 12.10.2021**
  - Apache releases Log4j 2.15.0 for Java 8 users to address remote code execution vulnerability dubbed "Log4Shell" – CVE-2021-44228
  - SonicWall releases [11 new IPS signatures](#) to detect the exploitation of threats related to CVE-2021-44228
- 12.12.2021**
  - First Cobalt Strike Beacons observed
  - Botnets observed utilizing Log4j to expand network
- 12.13.2021**
  - Apache releases Log4j 2.16.0 for Java 8 users to address RCE vulnerability (CVE-2021-45046)
- 12.14.2021**
  - C.N.A Apache Software Foundation releases [CVE-2021-4104](#), urging users of end-of-life (EOL) Log4j 1.2 to upgrade to supported branch (Log4j 2.x)
  - Industry reports on Advanced Persistent Threat actors (APTs) testing exploitability of Log4j
- 12.17.2021**
  - Apache releases Log4j 2.17.0 to address denial-of-service (DoS) vulnerability (CVE-2021-45105)
  - CISA issues Emergency Directive 22-02 that requires U.S. federal civilian executive branch agencies to address Log4j vulnerabilities
- 12.20.2021**
  - Belgian Defense Ministry compromised via exploitation of Log4j
- 12.21.2021**
  - Joint cybersecurity advisory ([AA21-356A](#)) issued by CISA, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK)
- 12.28.2021**
  - Apache releases Log4j 2.17.1 to address remote code execution (RCE) vulnerability (CVE-2021-44832)



## Deploying Dridex

Not to be outdone, another cybercriminal group exploited Log4Shell to [infect vulnerable Windows devices with Dridex malware](#), a banking trojan often used to download other payloads, steal credentials and more.

## Log4j's Legal Implications

For those ignoring their patching responsibilities, the consequences stretch far beyond the possibility of cyberattack. On January 4, 2022, [the U.S. Federal Trade Commission issued guidance](#) stating that that failure to take reasonable mitigation steps "implicates laws including, among others, the [Federal Trade Commission Act](#) and the [Gramm Leach Bliley Act](#)."

Citing the [Equifax breach of 2017](#) — and the \$575 million settlement that resulted from the company's failure to patch — the Commission warned that it "intends to use its full legal authority to pursue companies that fail to take responsible steps to protect consumer data from exposure as a result of Log4j."

## Forging Ahead

Log4j has highlighted the imminent need to elevate our concepts of defensible architectures, moving away from relying solely on perimeter-based security and toward a contemporary defense-in-depth strategy.

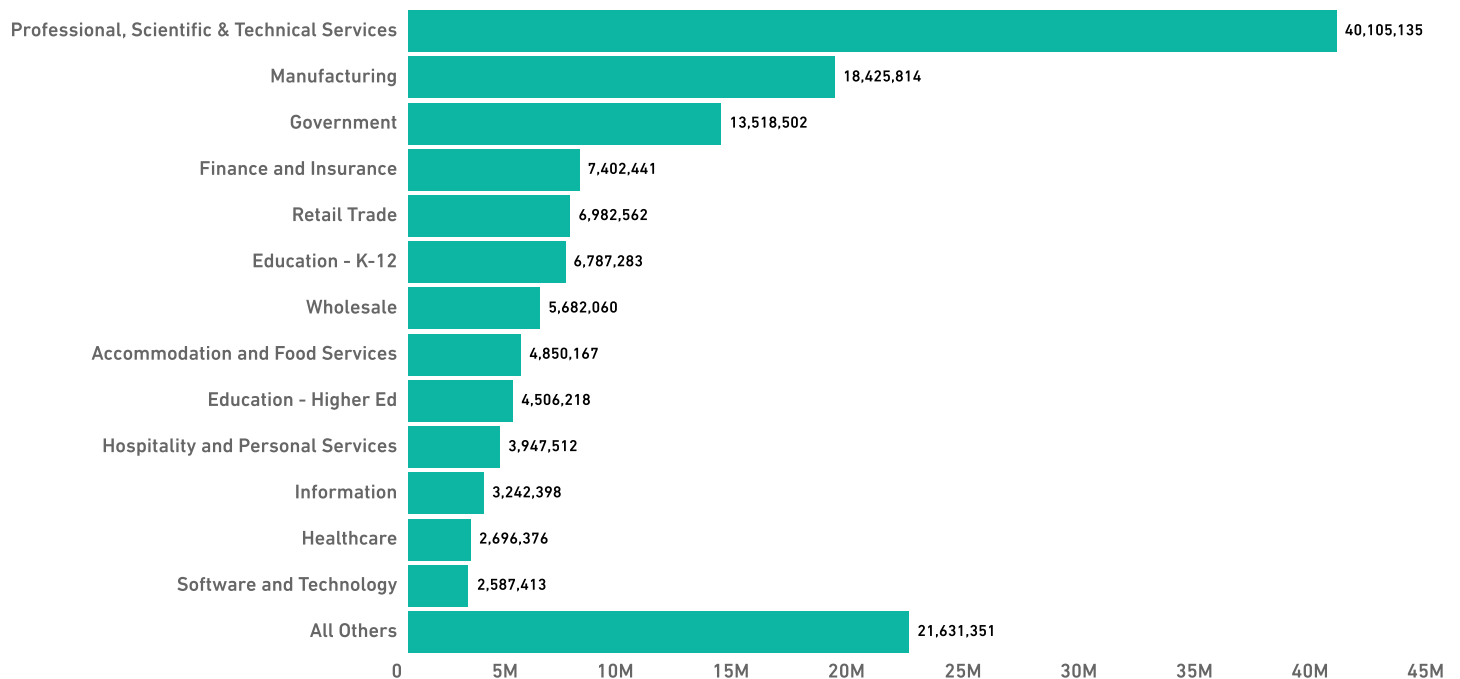
Such strategies must include integrating actionable threat intelligence to enhance visibility on supply-chain vulnerabilities across the code base and production environment, allowing security teams the opportunity to automate identification of CWEs and CVEs and orchestrate remediation across technology stacks.

These measures become increasingly crucial as supply-chain attacks increase, amplifying the impact of vulnerabilities, as we've seen with Log4j, Urgent/11, [Ripple20](#), [DNSpooq](#) and Amnesia:33.

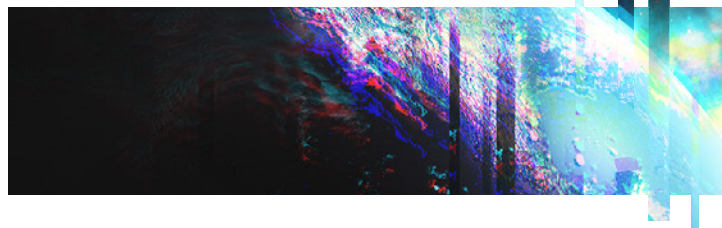
To reduce risk, an effort should be made to not only ensure visibility of dependencies and third-party code in your own technology stack, but also that of your vendors.

## Log4J Exploit Attempts By Industry

December 11, 2021 - January 31, 2022



# Business Email Compromise



## The Impersonators in Your Inbox

Why go to the trouble of employing obfuscation tools, launching multi-stage attacks, collecting credentials, exfiltrating data, encrypting endpoints or haggling over ransom amounts to get a payoff from your target, when you could just ask?

This is the basic premise behind Business Email Compromise (BEC) attacks, a form of cybercrime that's becoming increasingly common. [According to the FBI](#), nearly 20,000 of these attacks were reported in 2020 — likely a small percentage of the actual count. But despite being underreported, BEC attacks still cause **the most financial damage of any attack type, far more than even ransomware.**

### What are BEC Attacks?

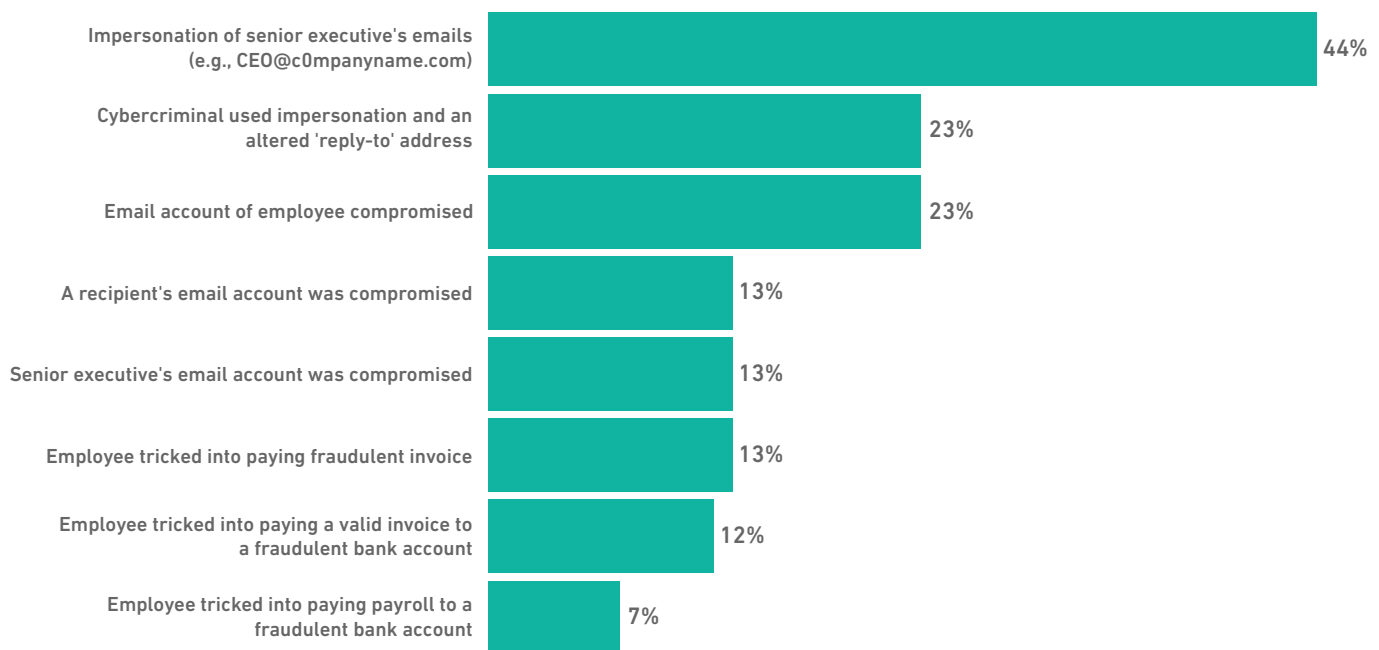
BEC attacks rely primarily on social engineering. While employees at any level can be targeted, the criminals almost

exclusively appeal to seniority to secure compliance. These attackers create email addresses that mimic those used by senior executives, use free services such as Gmail to create email addresses that appear to be an executive's personal account, or, less commonly, gain access to executives' actual corporate email accounts using phishing attacks or other means.

According to the Osterman white paper sponsored by SonicWall, ["How to Deal with Business Email Compromise"](#), once the attacker has a plausible email account from which to operate, they use social engineering tactics to, for example, request the target either divert payment on a valid invoice to the criminal's bank account, solicit payment via fake invoice or divert company payroll to a fraudulent bank account.

### Cybersecurity Incidents in 2021

Percentage of respondents experiencing each type of BEC attack



"How to Deal with Business Email Compromise," Osterman Research, Sponsored by SonicWall, January 2022

While BEC attacks fall under the umbrella of phishing, they don't typically include malware or malicious links. They don't have to: After all, who's going to say no to their CEO?

### BEC Attacks are Big Business

While simple, these attacks are both highly sophisticated and financially devastating. The FBI reported a total loss of [roughly \\$1.8 billion dollars in 2020](#) — and this is just from the attacks they were aware of.

Osterman's research estimates that 80% of organizations were targeted by at least one BEC attack in 2021. Mid-sized organizations, those with 500 to 2,500 email users, were even more likely to experience an attack: Nearly nine out of 10 saw an attack last year.

And these attacks are often successful. Nearly 60% of organizations surveyed reported being victims of a successful or almost successful BEC attack.

Roughly 40% of organizations said they had no BEC attacks that fell into these categories. But as these attacks become more common, organizations are becoming increasingly aware that they can no longer count on not being targeted as a defense strategy.

### Organizations Are Recognizing the Risk

The high number of successful attacks, coupled with growing news coverage of [the most devastating ones](#), is causing companies to reevaluate the risk posed by such attacks.

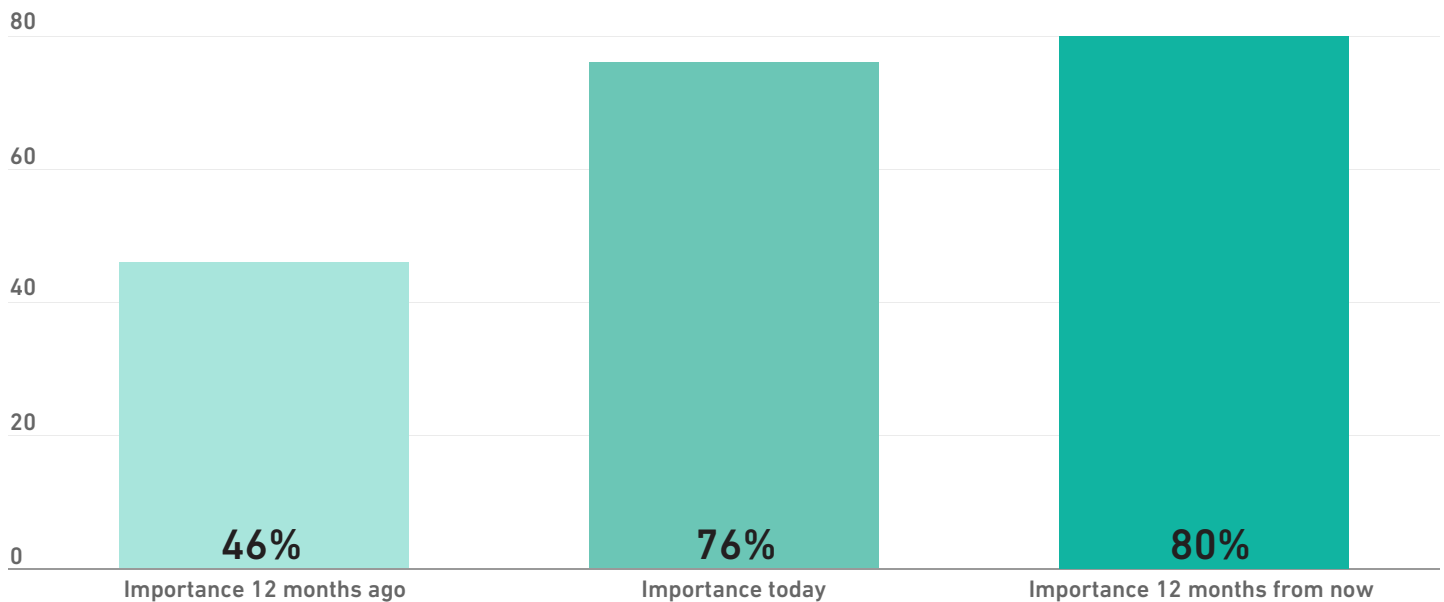
According to the Osterman survey, the number of organizations that claimed preventing such attacks was important to them grew by 30% in just one year, with further increases projected in the short term.

At the same time, respondents also said they lacked confidence in their existing protections and were unsure about their ability to safeguard funds, obtain help from insurance providers or law enforcement, or prevent these attacks from getting to highly targeted users in the first place.

Cybercriminals are aware that organizations are depending on cybersecurity technologies that were never designed to stop BEC attacks. But there are things you can do. **To learn more about BEC attacks, and what your organization can do to help prevent them, download our sponsored [white paper](#).**

## Importance of Protecting Against BEC Attacks: Three-Year View

Percentage of respondents indicating "important" or "extremely important"



\*How to Deal with Business Email Compromise." Osterman Research, Sponsored by SonicWall, January 2022



# Key Findings from 2021

▽ 4%



## Malware May be Headed for a Rebound

Malware was down 4% in 2021, marking both a third-straight year of decrease as well as a seven-year low. But there may be trouble on the horizon.

[READ MORE ON PAGE 19.](#)

△ 105%



## Ransomware's Savage Reign

In 2021, SonicWall threat researchers observed 623.3 million attacks globally. This total marked a 105% increase over 2020 and more than triple the number seen in 2019.

[READ MORE ON PAGE 29.](#)

△ 19%



## Cryptojacking: Bigger than Ever

Cryptojacking in 2021 rose 19% globally to 97.1 million — the most attacks that SonicWall Capture Labs threat researchers have ever recorded in a single year.

[READ MORE ON PAGE 40.](#)

△ 65%



## RTDMI Gets Smarter, Faster, Better

In Q4, RTDMI found more never-before-seen malware variants than in any quarter since its introduction in 2018. A total of 442,151 never-before-seen malware variants were identified in 2021, a 65% increase year-over-year.

[READ MORE ON PAGE 50.](#)

## Key Findings from 2021

△ 6%



### IoT Malware Shows Signs of Stabilizing

IoT malware volume rose 6% in 2021, totaling 60.1 million hits by year's end. This increase represents a leveling off compared with 2019 and 2020, when these attacks rose 218% and 66%, respectively.

[READ MORE ON PAGE 57.](#)

▽ 28%



### Malicious Intrusions Down by Nearly a Third

While total intrusions were up in 2021, the number of malicious intrusions fell 28%, from 16.4 billion to 11.9 billion.

[READ MORE ON PAGE 47.](#)

△ 167%



### Encrypted Threats Show Triple-Digit Increase

Encrypted threats climbed to 10.1 million attacks in 2021 — a 167% increase year-over-year.

[READ MORE ON PAGE 45.](#)

! 2FA



### Beware Authentication Fatigue

HTML phishing scams have begun launching realistic-looking login forms, relying on muscle memory developed during repeated daily logins to steal credentials.

[READ MORE ON PAGE 54.](#)

△ 52%



### Malicious Office and PDF Reverse Course

In 2021, the use of malicious Office files fell by 64%, while malicious PDFs rose 52%. This represents a significant reversal from 2020's trends.

[READ MORE ON PAGE 53.](#)

# Malware



## Malware May Be Headed for a Rebound

Total malware continued to drop in 2021, falling 4% year-over-year to 5.4 billion hits, according to SonicWall Capture Labs threat data. This represents both the third-straight year of decrease, as well as a seven-year low — but a closer look at the data shows this trend may be shifting.

A year-over-year decrease in malware is always good news. But keep in mind that yearly data is often the last place that trends appear. Think of ripples in a pond: the small areas (in this case, monthly or quarterly totals) are affected before the larger areas. And, unfortunately, a more detailed look at the 2021 data reveals a number of warning signs.

Since 2019, malware volume has been falling globally, from 5.1 billion in the second half in that year, to 3.2 billion in the first half of 2020, to 2.4 billion in the second half of 2020.

But in June 2021, SonicWall Capture Labs threat researchers noted that malware in the first half of the year had gone

up, rebounding to 2.5 billion (though it was still down 22% year over year.)

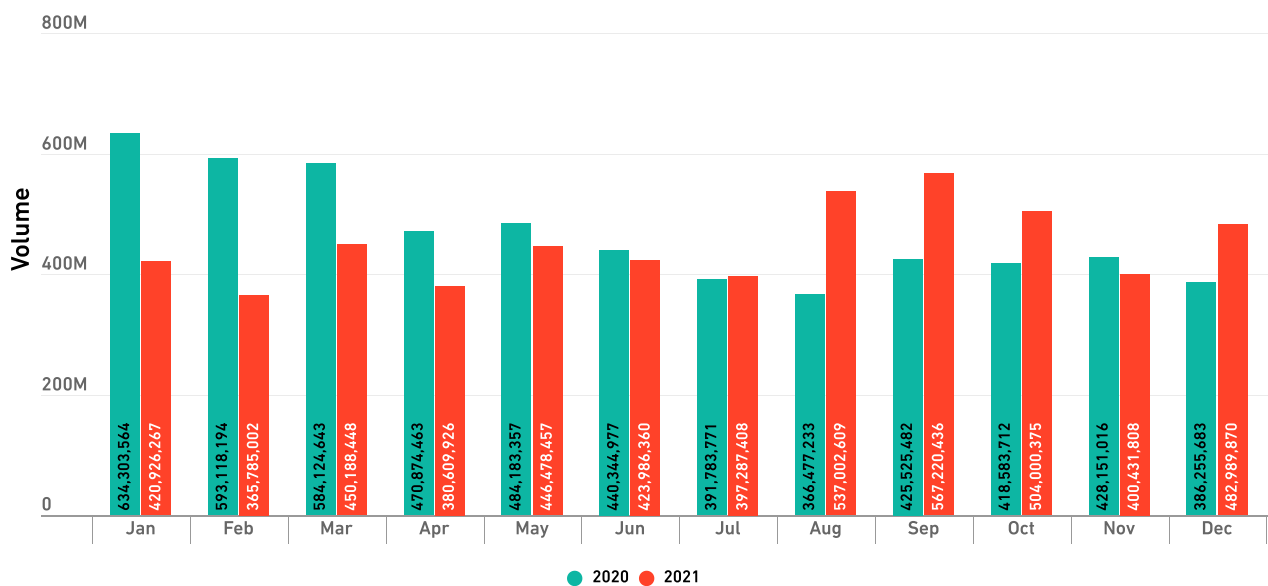
Unfortunately, the full-year data revealed this wasn't an anomaly. In the second half of 2021, malware rose even higher, reaching 2.9 billion.

In other words, while yearly data is still indicating a downward trend, looking at the data a half-year at a time shows that, for both halves of the year, the use of malware was trending back up.

Ominous bellwethers appeared in the monthly data, as well. In August, malware volume soared to 537 million, breaking the 500 million mark for the first time since March 2020.

The average monthly malware volume was roughly 80 million higher in the second half of 2021 than in the second half of 2020 — and unfortunately this wasn't due to one anomalous month, but to sustained higher volume overall.

### Global Malware Volume







## 2021 Malware Volume: Changeabout — or Just a Correction?

In the 2021 SonicWall Cyber Threat Report, we delivered 2020's malware numbers with a caveat: The rapid and unexpected shift to remote work had caused a decrease in visibility for corporate networks, and by extension cybersecurity vendors, SonicWall included.

But while the pandemic has led to remote work becoming an accepted option among those who are able, employees still returned to the office in droves in 2021, particularly in the second half.

[According to Bloomberg](#), between Sept. 18 and Oct. 16, the number of Londoners riding the tube was triple what it had been in March. And in December 2021, occupancy

levels in New York City offices hit a pandemic high, up significantly from January.

The question now becomes: Are we seeing more malware because we're *seeing* more malware, as people have been coming back into the office and companies have begun retooling their cybersecurity solutions to ensure visibility of a remote workforce?

Or are we seeing more malware because there *is* more malware — because, even though cybercriminals are focusing less on trojans, carders and banking info stealers that require more work down the line, the increase in ransomware is more than making up for it? Only time will tell.

---

## Malware by Region

Another worrying sign appears in the regional data. In 2020, malware volume decreased year-over-year in every single region. In 2021, it was only down in one region, and it wasn't down by much: North America saw a 9% decrease, sinking to 3.1 billion.

Europe and Asia were not as fortunate. Malware in Europe rose 35% year over year, to a total of 1.3 billion. In May, the number of malware hits there passed 100 million for the first time since 2020, and they stayed above this point for the rest of the year. In Asia, malware volume increased 27%, a significant reversal from the 53% year-over-year decrease recorded in 2020.

## What is Malware Spread?

SonicWall recorded 2.9 billion malware hits in the U.S. in 2021 — nearly six times the next-highest ranked (U.K., with 492 million). So why aren't these countries the riskiest?

Malware totals are useful in calculating trends, but they're of limited utility when determining relative risk: They ignore factors such as size, population, number of sensors and more.

To find out the odds that an organization in a particular area will see malware, we use the malware spread percentage — a calculation of what percentage of sensors saw a malware attack.

If we think of malware volume as being similar to the total amount of rainfall in a given region, then malware spread percentage could be compared to the probability of precipitation, or "chance of rain."

Think of it this way: Annual precipitation numbers can be useful in determining whether your area has seen more rain than it did last year, but they don't tell you whether your umbrella will see heavier use than your tube of SPF. Like the "chance of rain," malware spread percentage considers a variety of additional factors to provide a more meaningful risk assessment.



## Malware Spread by Country

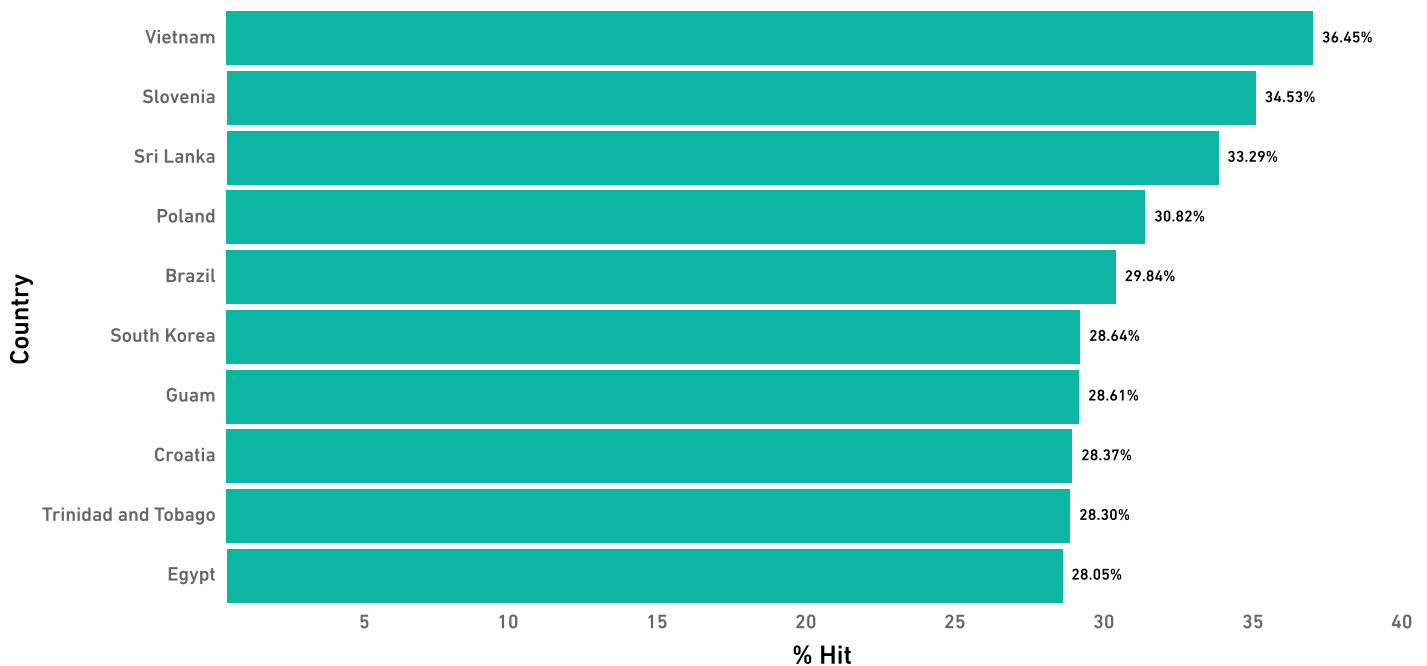
The U.S. and the U.K have the highest malware volume. But based on malware spread data, we can see that an organization is actually most likely to see a malware hit in Vietnam, where malware spread in 2021 was 36.4%.

Interestingly, South Korea — where malware spread was the highest last year, at 51.4% — saw a huge drop in malware spread in 2021. South Korea is now No. 6 on the list, with a malware spread of 28.6%.

If you want to minimize your chances of being hit by malware, head to Luxembourg: only 6.6% of SonicWall sensors there recorded malware hits.

**An organization is actually most likely to see a malware hit in Vietnam, where malware spread in 2021 was 36.4%.**

### 2021 Malware Spread | Top 10 Countries



## 2021 Malware Spread | Top 10 Riskiest States

In 2020, California had the highest malware of any state, with a volume of 408.3 million — nearly 70% more than the next-highest state. But in 2021, the number of hits in that state fell by 28%, to 293 million.

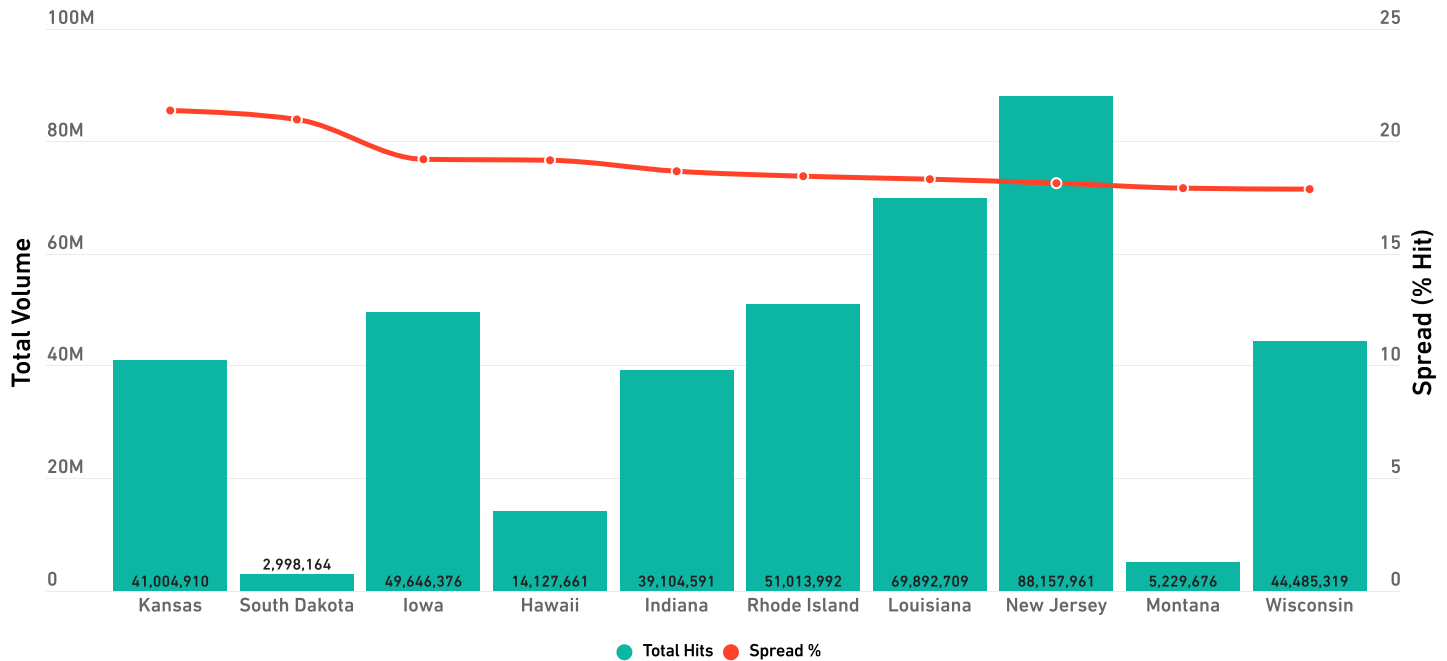
Rising to fill its place was Florida, which had more than twice as many hits in 2021 as California, with a total of 625.4 million. (New York, with 306.8 million hits, came in second.)

But if these three states have so much malware, are they the most dangerous? As it turns out, no: None even made the top 10. (California was actually fifth from the bottom.)

So which state is the riskiest? For the second year in a row, it's Kansas, where roughly 21.4% of SonicWall sensors saw a malware hit. Fortunately for those in the Sunflower State, however, this is down from the 26.7% recorded last year. (In other words, slightly more than 1 in 4 saw a hit in 2020; in 2021 it was closer to 1 in 5.)

At the other extreme, in Maine only 14.7% of sensors logged an attempted malware attack.

## 2021 Malware Spread | Top 10 Riskiest U.S. States



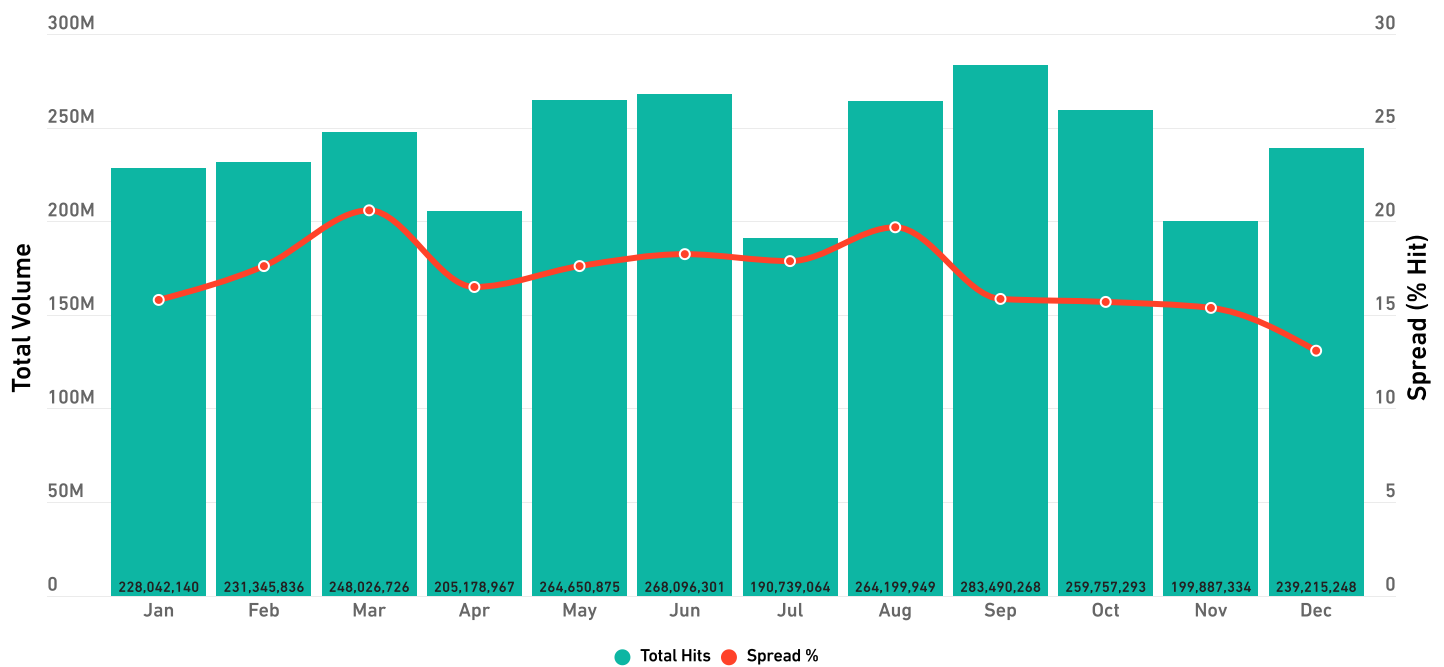
# Malware Risk by Country

In a relatively small sample size of eight countries, there's still a huge variation in outcomes. But one thing remained remarkably consistent regardless of where the country was located, what its total malware volume was, or how the overall trendlines fell.

When looking at SonicWall's exclusive malware spread percentage data — which tells us how widespread malware

is in a given region (see sidebar) — every country studied had a lower malware spread percentage in December than in January. While a cursory look at the trendlines shows how quickly these levels can rise and fall, at least these countries are going into 2022 in a better position than where they started 2021.

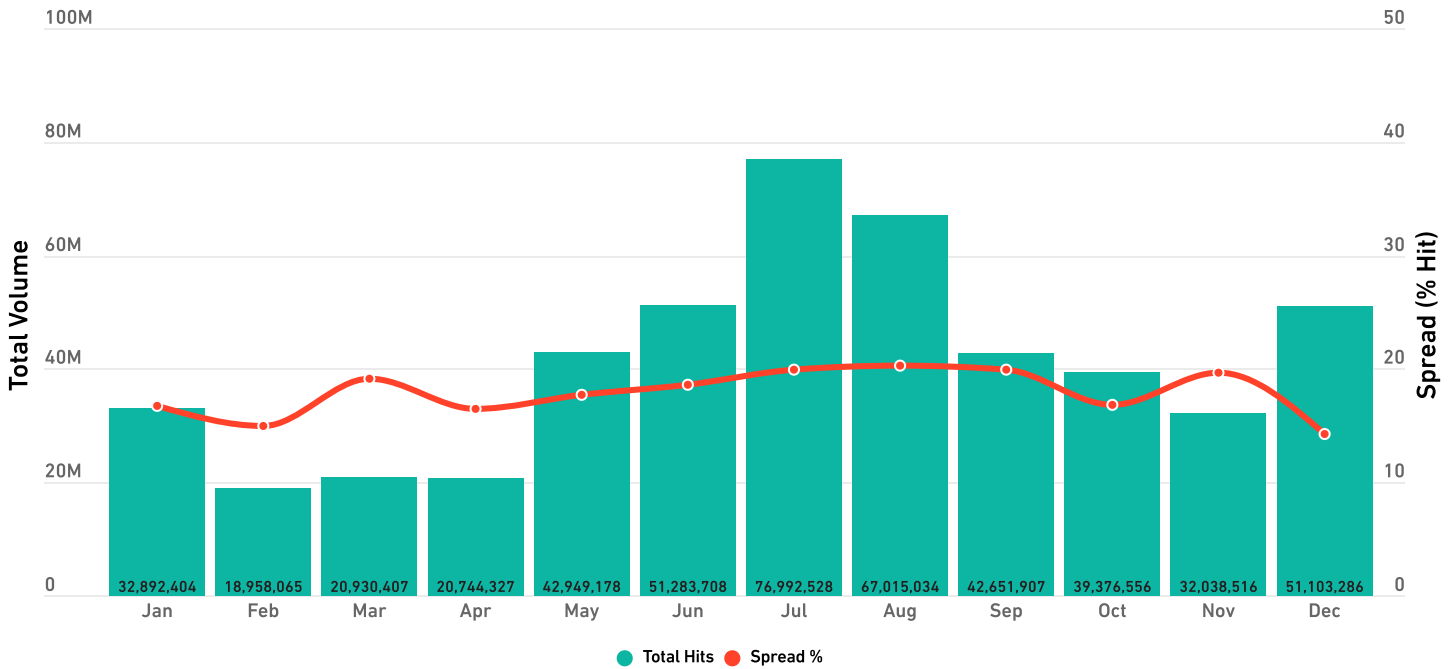
## 2021 Malware Attacks | United States



While U.S. malware fell much more slowly in 2021 than in 2020, malware spread fell a bit faster.

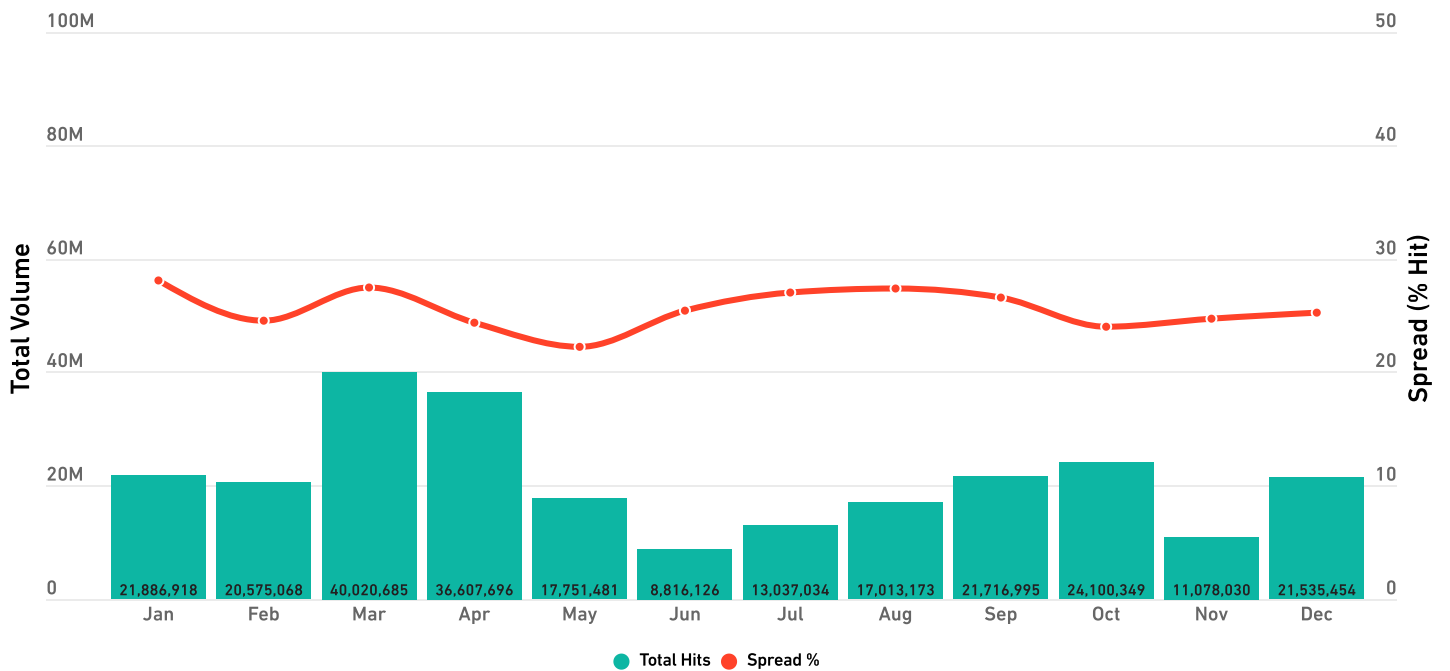


## 2021 Malware Attacks | United Kingdom



In the UK, the number of malware hits was up 48% year over year. Volume was highest in July — the opposite of the U.S., which saw its lowest point that month.

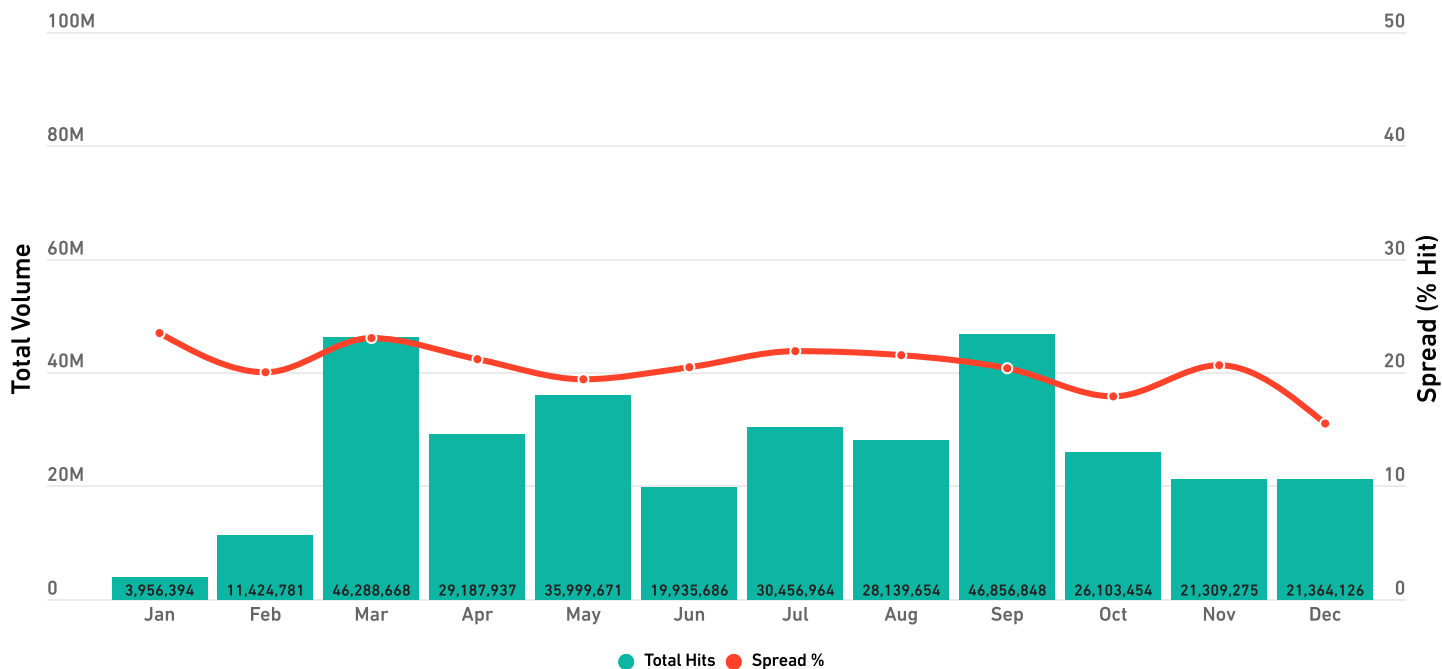
## 2021 Malware Attacks | India



India saw a 41% increase in malware volume in 2021, with nearly a third of the year's total occurring in March and April.

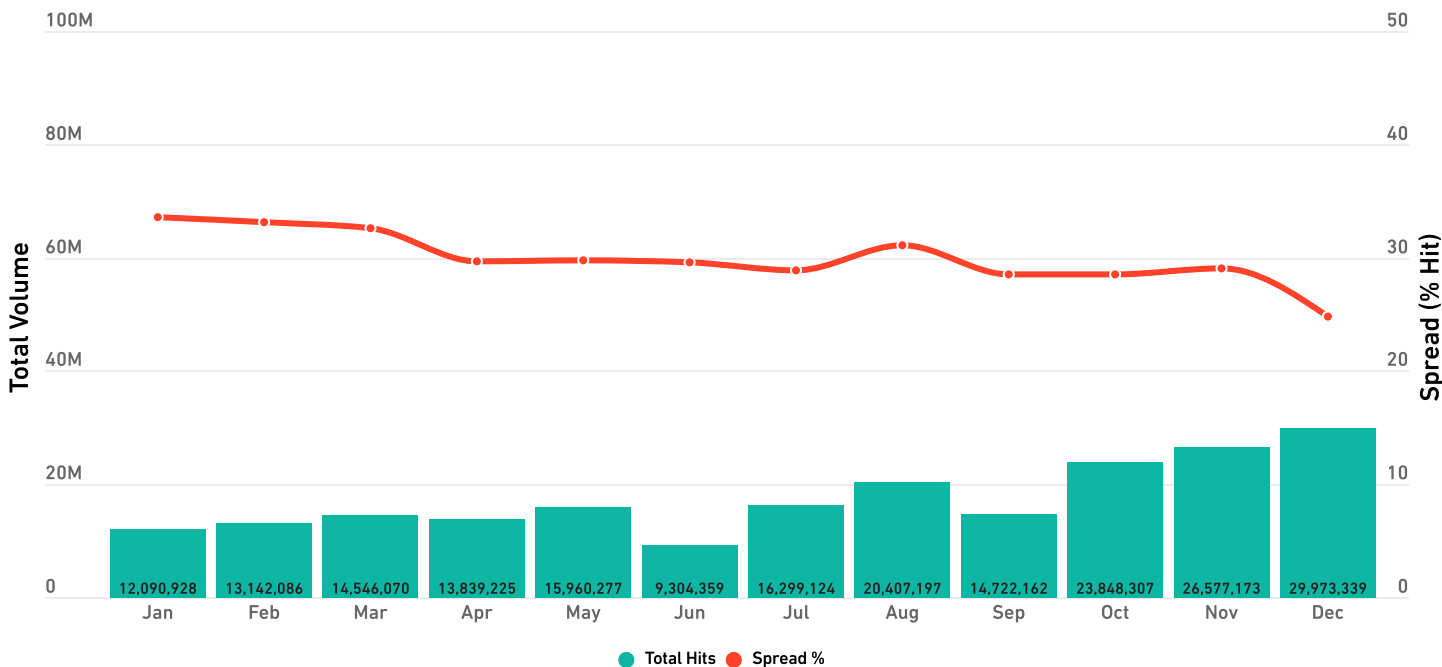


## 2021 Malware Attacks | Germany



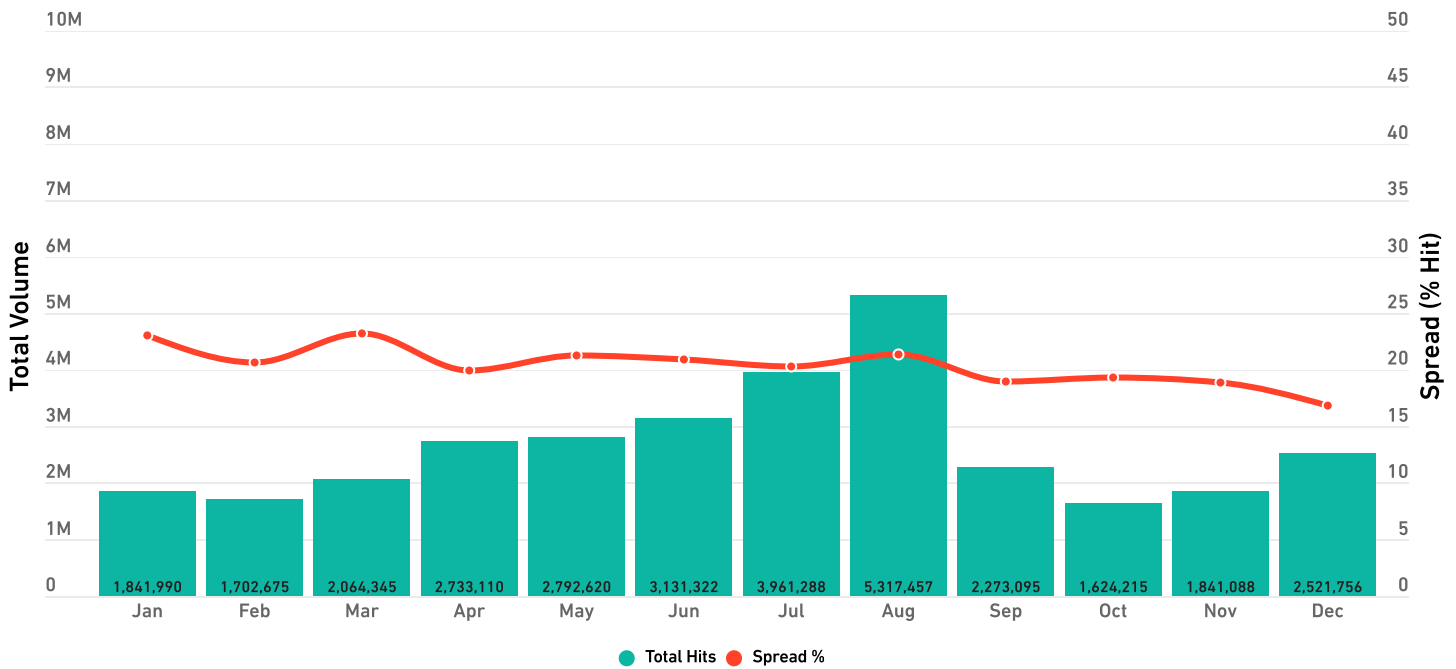
In Germany, malware volume skyrocketed an astounding 597% year-over-year. The biggest increase was from February to March, when malware volume jumped from 11.4 million hits to 46.3 million hits — an increase of 306%.

## 2021 Malware Attacks | Brazil



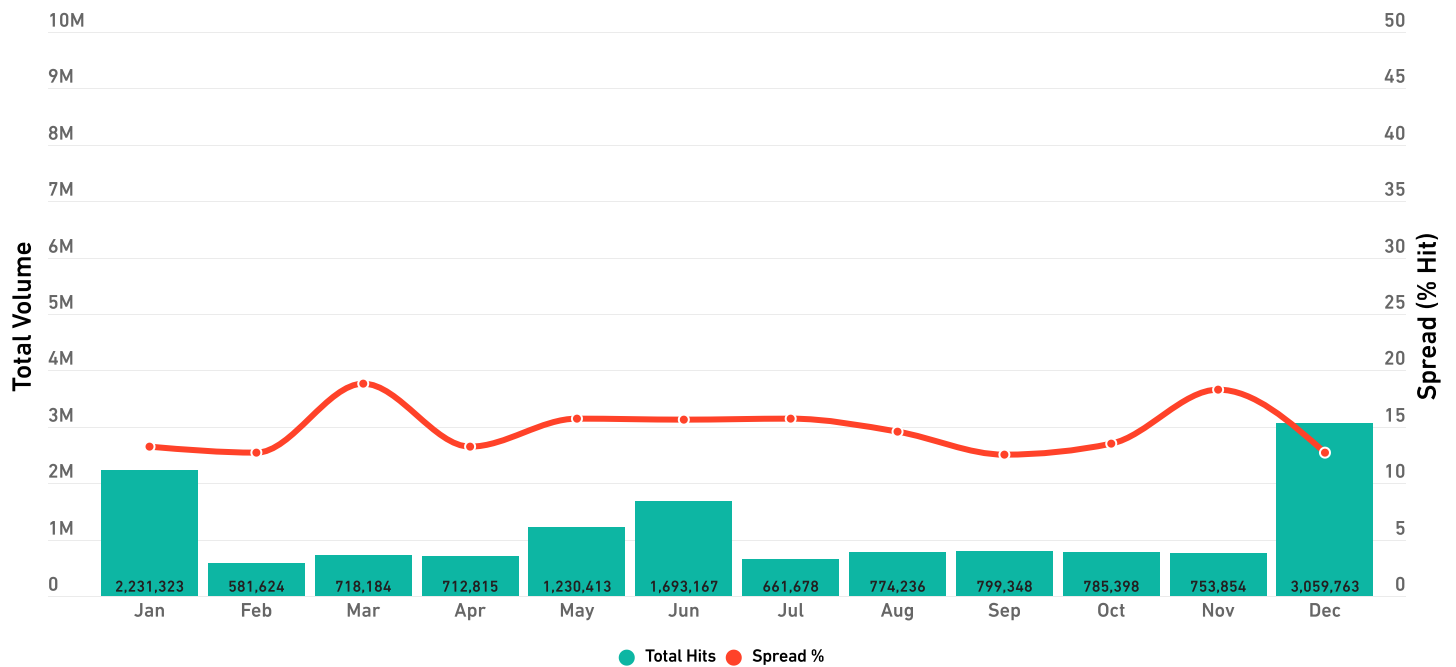
Brazil was the only one of the eight countries studied to have malware volume heavily concentrated in Q4: Malware volume for that quarter was 80.4 million, compared with 51.4 million in Q3, the next-highest quarter. Malware volume in Brazil was up 61% overall.

## 2021 Malware Attacks | Mexico



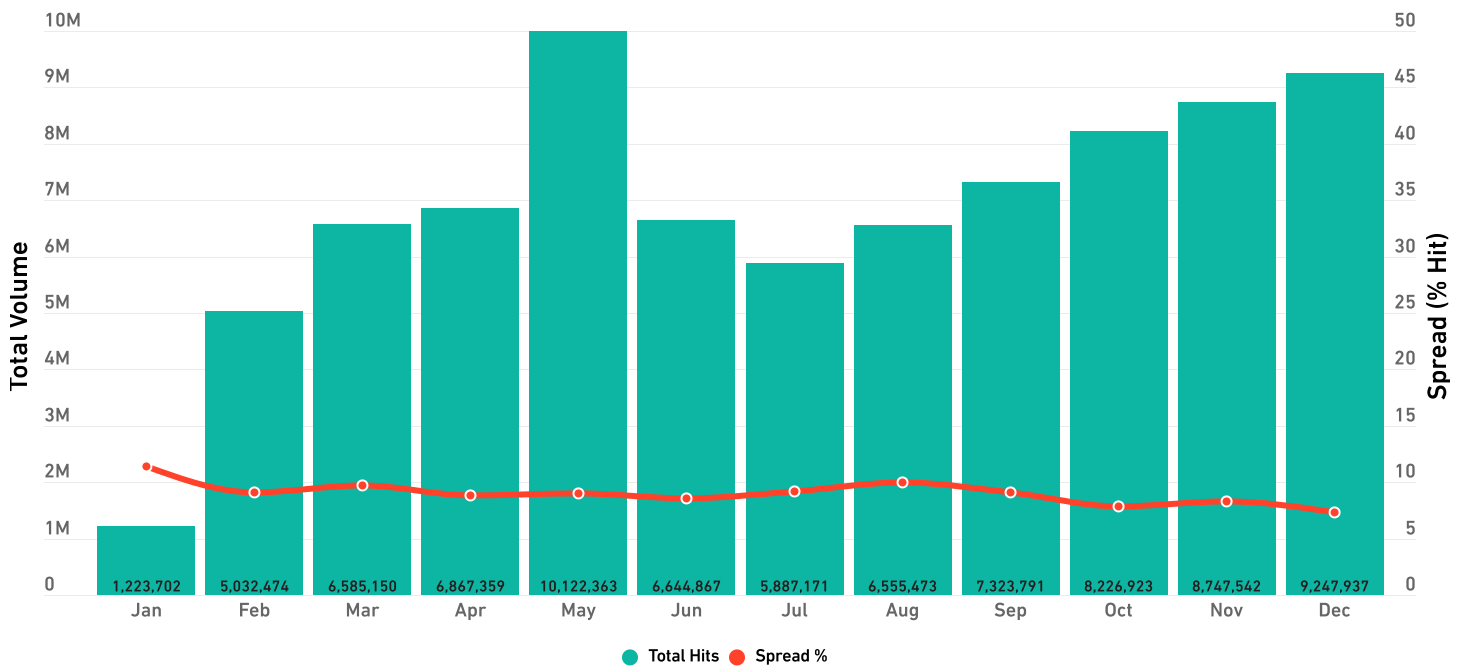
While malware in Mexico was up 78.5% from 2019, most of that change actually occurred in 2020, when Mexico was one of the only countries to see an increase. From 2020 to 2021, malware increased only 3%.

## 2021 Malware Attacks | Japan



Malware volume in Japan was up 64% year over year, handily undoing the 12% drop the country experienced in 2020. December saw the biggest increase: Between November and December, volume jumped 287.5%.

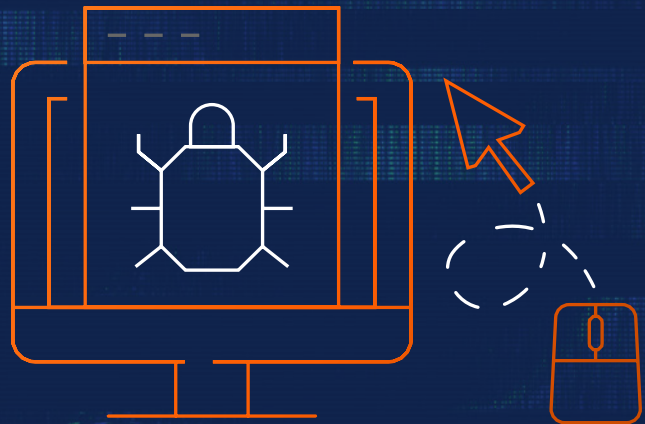
## 2021 Malware Attacks | United Arab Emirates



In UAE, January had significantly less malware than any other month, with less than a quarter the number of hits as the next-lowest month (February). Overall, malware volume in UAE was up 333%.

## Top 10 Most Common Malware Filenames

1. Confirma-Webmail.bat 19%
2. QUOTATION.exe 11%
3. SOA.exe 10%
4. PURCHASE ORDER.exe 10%
5. Invoice.exe 7%
6. PO.exe 6%
7. New order.exe 6%
8. DHI\_document.doc.exe 5%
9. Product-inquiry\_PDF.exe 5%
10. Payment.exe 5%



# Malware by Industry

Two industries saw large spikes in malware in 2021: healthcare (121%) and government (94%).

These weren't the industries likeliest to see a malware hit, however. Once again, the industry with the highest percentage of customers targeted was education; once again, this held for the entire year; and once again, it wasn't even close.

An average of 22.5% of education customers were targeted by malware in any given month, compared with government at an average of 19.6%. Retail and healthcare were essentially tied, with 16.4% and 16.3%, respectively.

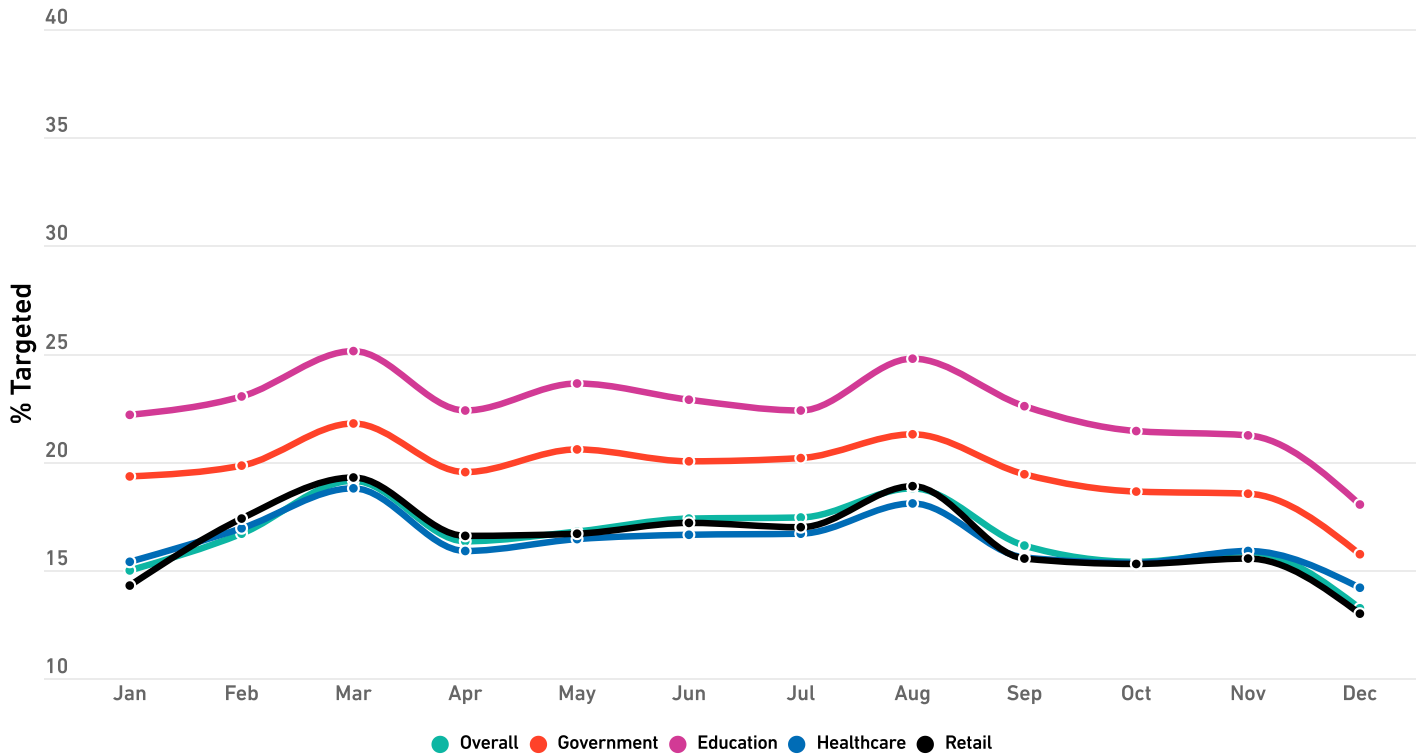
The industry trends for malware shared a lot in common. In all industries, the percentage of customers targeted peaked twice, once in March and again in August.

And while both January and December were both consistently low, December had the lowest percentage of

**An average of 22.5% of education customers were targeted by malware in any given month, compared with government at an average of 19.6%.**

customers targeted all year across every industry studied. While the trends in malware as a whole suggest we temper our expectations, this data shows at least one malware metric is headed in the right direction.

### % of Customers Targeted by Malware





# Ransomware



## Ransomware's Savage Reign

When ransomware started to spike in the second half of 2020, it set off alarm bells within the cybersecurity community and around the world.

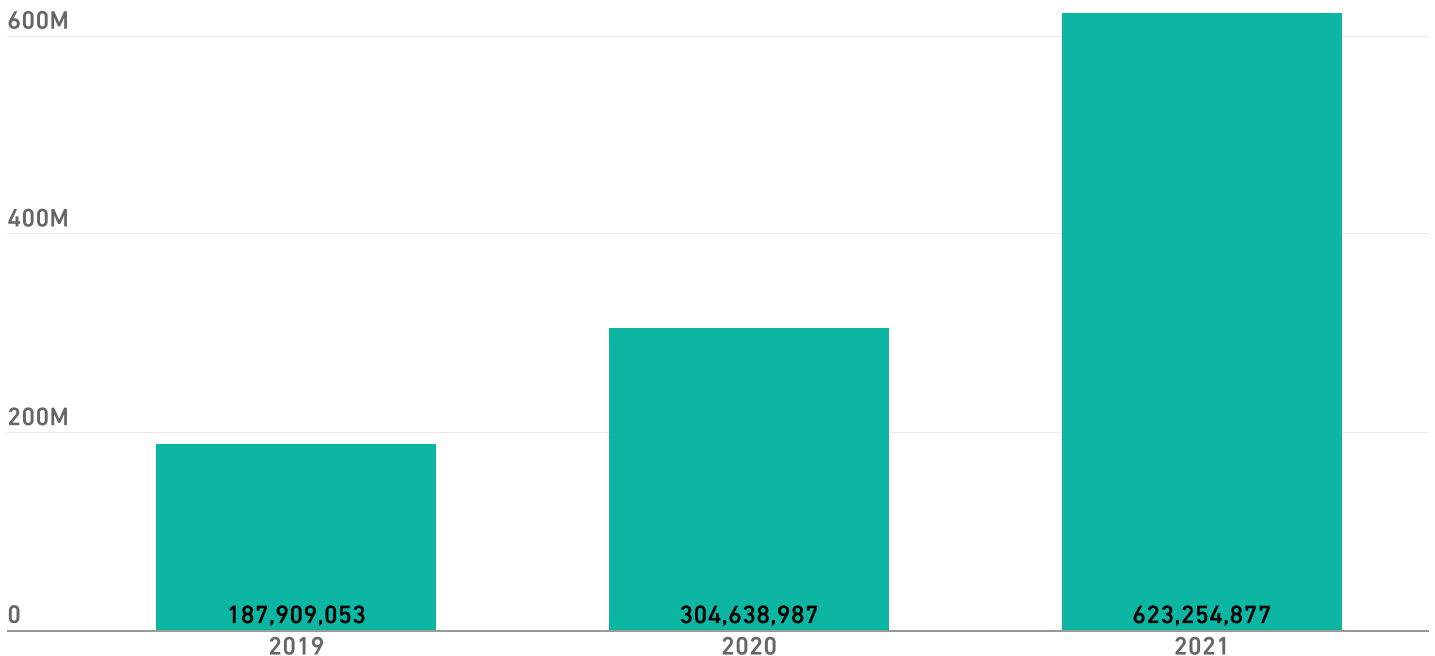
But the ransomware volume in the worst month of 2020 — 37.8 million, observed in November — barely exceeded the *lowest* point for 2021, and we would see that number more than double by year's end.

In what would become one of the worst years for ransomware ever recorded by SonicWall, attack volume rose 105% to a staggering 623.3 million. This represented an average of 2,170 ransomware attempts per customer, and nearly 20 ransomware attempts *every second*.

**Nearly 20 ransomware attempts every second.**

A 105% increase year-over-year is worrisome enough. But to truly understand ransomware's meteoric rise, it helps to compare 2021's ransomware volume to 2019 as well. Ransomware has risen a mind-blowing 231.7% since 2019. While 2021's high-water mark was more than double that of 2020, it more than *tripled* the ransomware volume in the worst month of 2019 (May, which saw a ransomware volume of 25 million).

Global Ransomware Volume by Year



The number of hits per month started off strong in January, when ransomware volume reached 43.1 million, besting 2020's worst month (Nov. 2020, with 37.8 million attempts) right out of the gate. But ransomware, like the year itself, had only just gotten started.

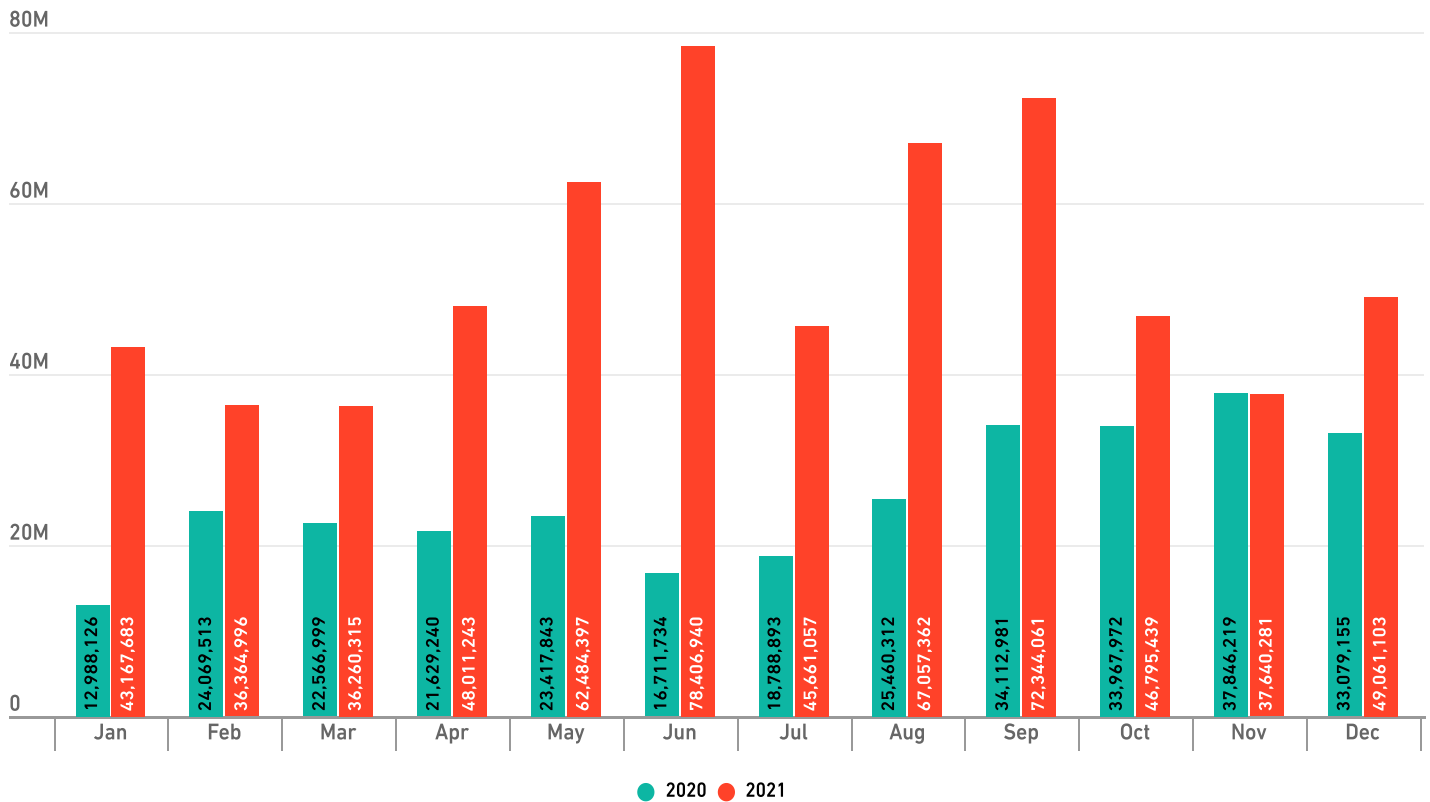
In June, ransomware reached a high of 78.4 million — a level higher than three out of four *quarters* in 2020.

In fact, with 304.7 million attempts, the first half of 2021 had more ransomware than all of 2020 — but the second half would prove to be even worse, reaching 318.6 million.

The year's only bright spot came in Q4: Ransomware hits for the quarter dropped 50 million from their sky-high Q3 totals, near where the year started.

**In fact, with 304.7 million attempts, the first half of 2021 had more ransomware than all of 2020 — but the second half would prove to be even worse, reaching 318.6 million.**

## Global Ransomware Volume



## Ransomware by Region

In North America, ransomware rose 104%, just under the 105% average increase worldwide. But other regions had it much worse. In Asia, ransomware rose 122%, and in Europe, the number of hits climbed even more, rising 175% year over year.

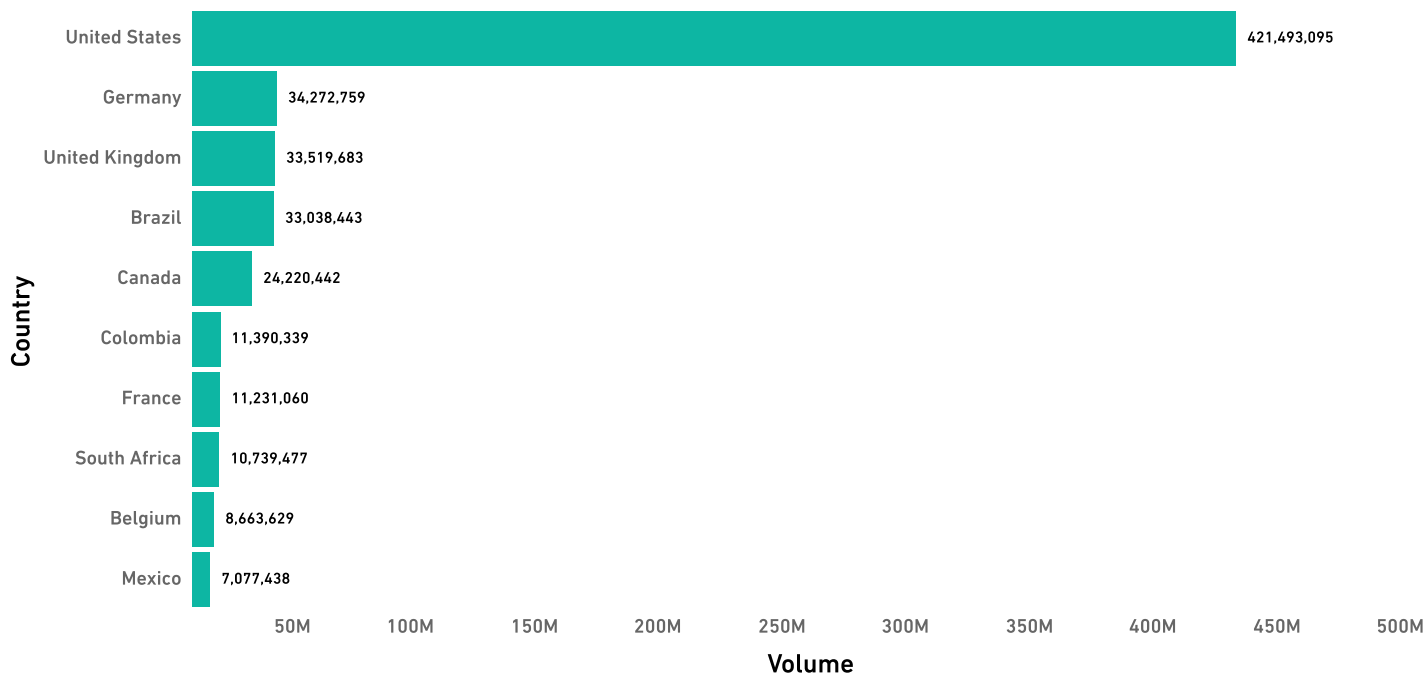
To put Europe's increase in perspective, consider that it had been at least five years since monthly ransomware totals had surpassed 10 million — but in June 2021, they reached 10.4 million. The month of September, however, had more than double this number at 22.3 million attempts — more than half as many as in the *entire year* of 2020.

Until 2021, the countries that experienced the most ransomware were the U.S. and the U.K. Both saw large year-over-year increases, with ransomware volume in the U.S. rising 98% to 421.5 million and ransomware in the U.K. rising 227% to 33.5 million.

**In Asia, ransomware rose 122%, and in Europe, the number of hits climbed even more, rising 175% year over year.**

But Germany saw a far higher increase in ransomware volume. The number of ransomware hits there rose to 34.3 million in 2021, a mind-blowing 3,256% year-over-year increase and enough to unseat the U.K. as second in line, according to SonicWall data.

### 2021 Ransomware Volume | Top 10 Countries





## Notable Ransomware Identified in 2021

A number of new ransomware developments were observed in 2021. Here are some of the most noteworthy:

### JANUARY

Jan. 14 Babuk Ransomware Actively Spreading in the Wild

### FEBRUARY

Feb. 5 Cukiesj, a Paradise Ransomware Variant, Demands Over \$50k for File Retrieval

Feb. 26 Parasite Ransomware Targeting French Users Actively Spreading in the Wild

### MARCH

March 5 Lotus Ransomware Charges 1 Bitcoin; Multi-PC Discount Possible

### APRIL

April 9 Uniwinncrypt Ransomware Charges Over \$550k for File Recovery

April 16 Ransomware Uses Discord for C2 Communications

April 23 Ransomware-as-a-Service Actively Spreading in the Wild

### MAY

May 27 Conti Operator Demands \$20M from Victim; Faces Litigation Backlash Instead

### JUNE

June 11 Another Ransomware Possibly Belonging to the REvil Ransomware Group Seen Actively Spreading in the Wild

### JULY

July 1 Snoopdog Ransomware Charges 36k in Bitcoin for Recovery; 20% Discount Negotiable

July 6 Kaseya VSA Server Exploitation and Another Supply-Chain Ransomware Attack

### AUGUST

Aug. 12 Nooa Ransomware Seeks Out Your Crypto Wallets and Passwords

### SEPTEMBER

Sept. 3 Lockbit 2.0, the Ransomware Behind the Accenture Breach

### OCTOBER

Oct. 1 Atomsilo Hits Large Brazilian Company in \$1M Double Extortion Scheme

### NOVEMBER

Nov. 5 Foxyy RaaS Released; Decryption Key and Function Present in Sample

### DECEMBER

Dec. 3 WordPress Websites Plagued by Fake Ransomware

Dec. 17 GarranDecrypt Ransomware Operator Charges \$5K for Decryption; Price Negotiable

Dec. 29 Github Hosted Android Ransomware Being Misused in the Wild

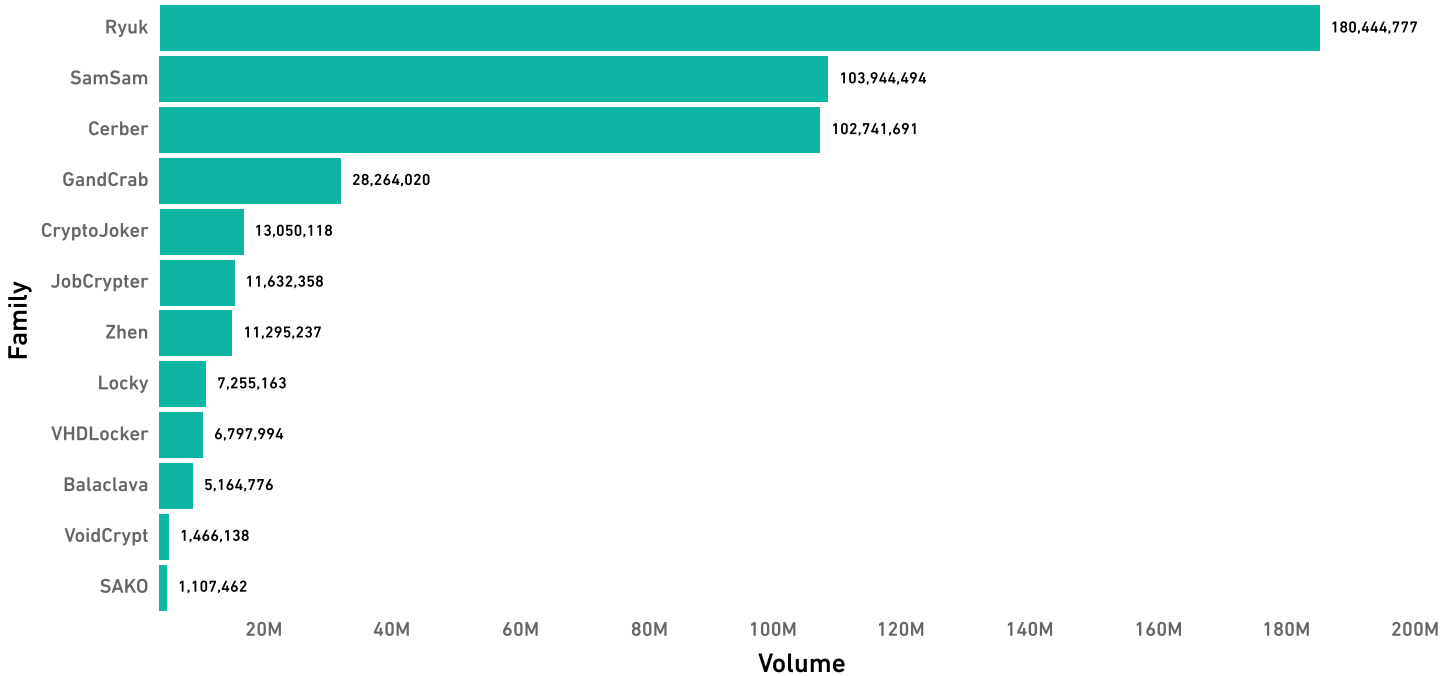


# Top Ransomware by Signature

SonicWall Capture Labs threat researchers recorded hits from roughly 1,000 different ransomware signatures in 2021 and more than 300 ransomware families.

However, three families accounted for 62.1% of all ransomware in 2021, and they were the same frontrunners as last year: Ryuk, SamSam and Cerber.

### 2021 Ransomware Volume | Top 10 Families



## Ryuk Runs Rampant

In 2021, SonicWall Capture Labs threat researchers recorded 180.4 million hits of Ryuk, a 64% increase year over year. This accounted for roughly 30% of all ransomware attempts observed for the year, down from 36% of all ransomware in 2020 (As we'll see later, the slack was largely picked up by Cerber and SamSam).

In other words, while Ryuk's *share* of all ransomware attacks fell during 2021, this decline is overshadowed by the fact that Ryuk is still on top, and is still very much on the rise.

For most of the year, Ryuk levels in 2021 exceeded those in 2020. Volume peaked in June, setting a new record of 24.2 million hits — roughly 9.32 Ryuk hits each second.

The fact that there were fewer instances of Ryuk in the second half of the year than the first is undeniably a good sign. But the emergence of new capabilities (see below) is evidence that threat actors are committed to Ryuk, so we'll likely continue seeing this ransomware family at or near the top of the list for the foreseeable future.

## Ryuk: From Trickbot and Emotet to Worms and BazarLoader

Once again, Ryuk was observed spreading primarily via phishing and spearphishing campaigns, but also entered

networks via compromised credentials or malware already active on a target's system, such as Trickbot and Emotet.

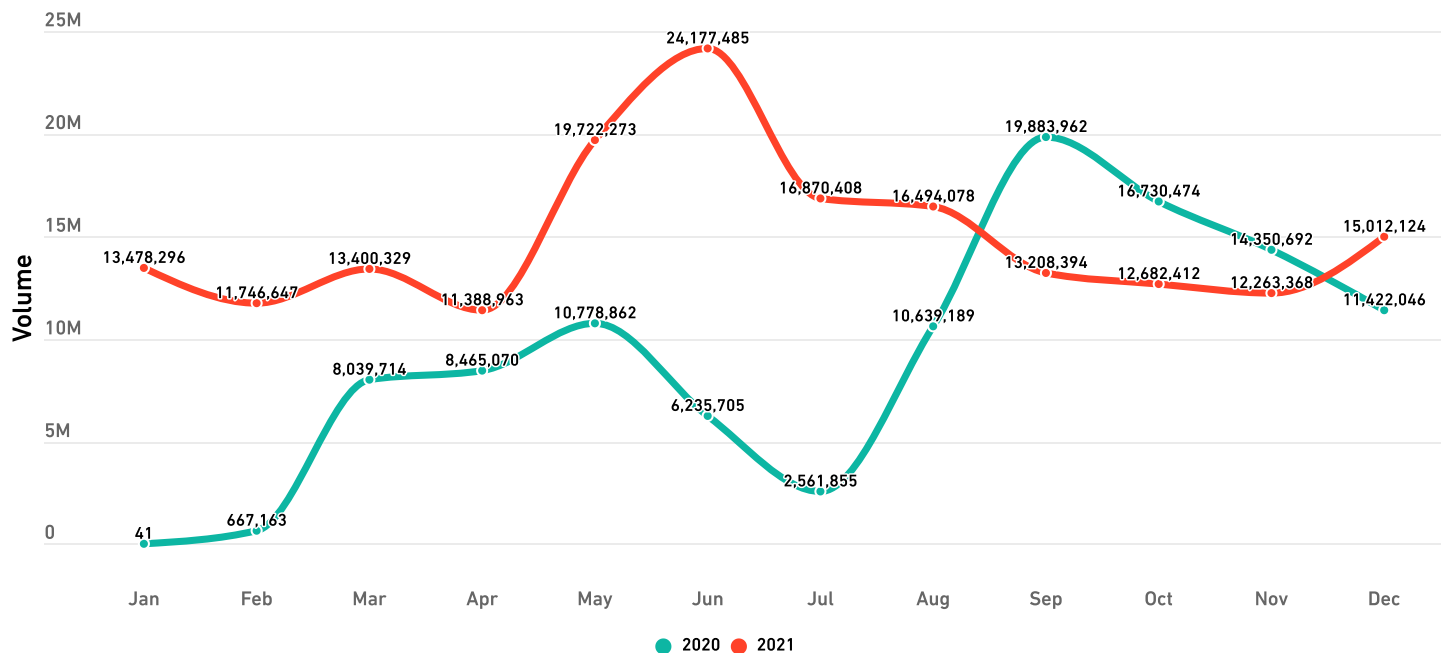
While Trickbot and Emotet have traditionally been attack vectors for Ryuk, both have had a rough couple of years. In 2020, a high-profile operation carried out by Microsoft and a number of other organizations [significantly disrupted Trickbot](#), and in early 2021, a collaboration between law enforcement and judicial authorities worldwide [took Emotet down](#). (Unfortunately, however, [both of these takedowns proved temporary](#).)

Perhaps seeing the need to diversify, Ryuk in September 2020 began to use BazarLoader for [more valuable targets](#) — a method that is costlier and more involved, but pays dividends in stealth.

In early 2021, a new "wormlike" Ryuk variant was [discovered by France's ANSSI](#). Previously, Ryuk lacked the ability to move laterally through networks — it relied on manual movement to spread. But the new version [is able to self-replicate, infecting new machines](#) without the need for human intervention.

Worse, because a privileged domain account is used, [the report states](#), neither changing the password nor disabling the account will help.

### Global Ryuk Ransomware Volume



## SamSam Skyrockets

SamSam, while still a distant second to Ryuk, showed spectacular growth in 2021. Ransomware in the SamSam family spiked 343% year over year, soaring from 23.5 million hits in 2020 to 104 million hits in 2021.

As a result, SamSam made up a much higher percentage of all ransomware in 2021 than in 2020: In 2020, 7.7% of all hits were SamSam, but last year that more than doubled to 16.7%

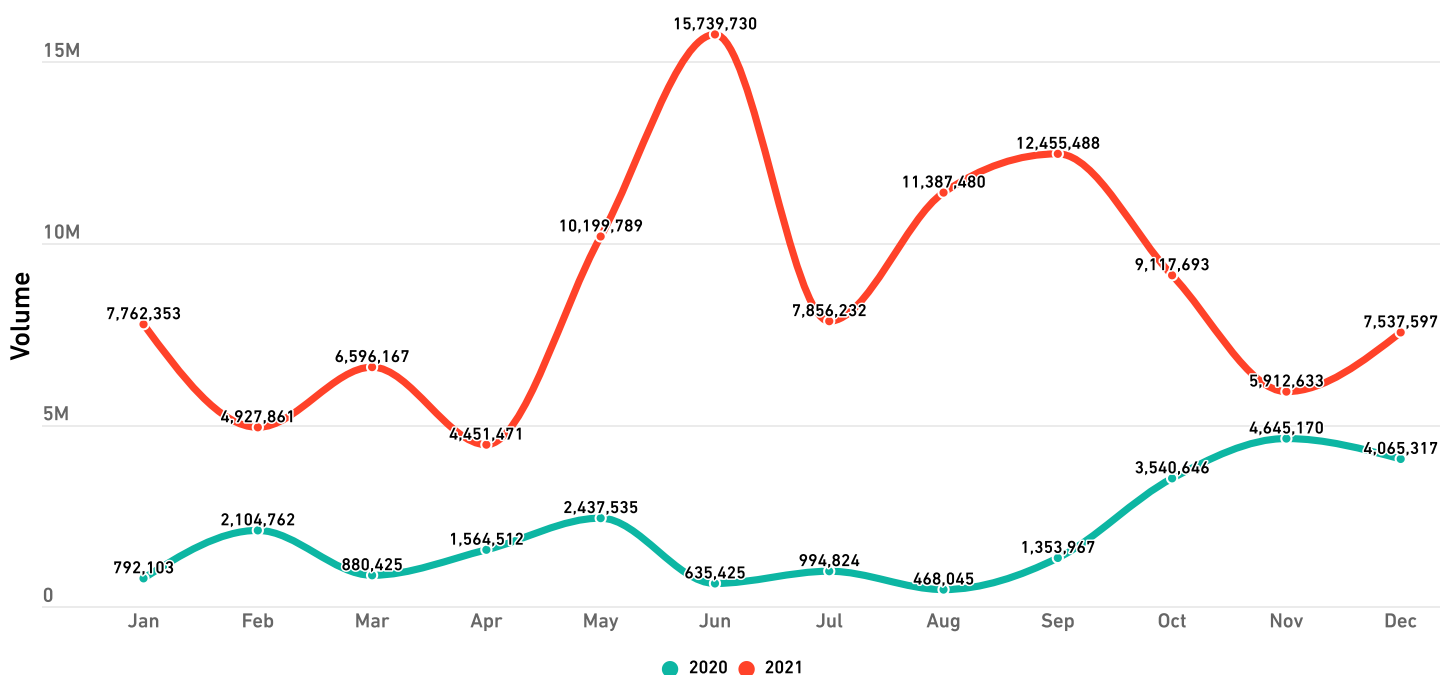
To put this increase in perspective, there was not a single month in 2021 where the volume of SamSam was lower than in 2020. Like Ryuk — and ransomware in general — SamSam volume peaked in June, setting a new record of 15.7 million attempts.

Unlike Ryuk, which is a well-known Ransomware-as-a-Service (RaaS), SamSam is not sold in the underground, but is instead developed privately and updated often. The group

**There was not a single month in 2021 where the volume of SamSam was lower than in 2020.**

behind SamSam [has a reputation for](#) scanning the internet looking for mentions on their attacks: once an attack is reported or cybersecurity vendors update their signatures, the group launches a new version. This high level of attention has helped ensure that SamSam could continue to operate successfully [for going on seven years.](#)

### Global SamSam Ransomware Volume



## Cerber Continues Climb

Before Ryuk soared to the top of SonicWall’s ransomware families rankings, there was Cerber. In 2019, Cerber made up 33% of all ransomware attacks recorded by SonicWall, but in 2020 it fell to roughly 13%.

Use of Cerber could be rebounding, however: In 2021, Cerber rose 158% year over year, and now makes up 16.5% of all ransomware hits recorded.

First developed in March 2016, Cerber was one of the first examples of the RaaS business model: The operators of Cerber [originally offered their ransomware](#) for a 40% cut of any ransoms paid. Cerber has been known to spread via exploit kits, malicious JavaScript attached to spam, infected websites, fake software downloads and malvertising.

## Five Years On: The (Continuing) Legacy of WannaCry

In February 2021, the U.S. Department of Justice (DOJ) [indicted three North Korean attackers](#) for their suspected role in spreading WannaCry. This infamous ransomware propagated through the EternalBlue exploit, which was developed by the U.S. National Security Agency, then stolen and leaked by a group called [the Shadow Brokers](#).

This group, through a series of ransomware attacks, extorted over \$1.3 billion in money and cryptocurrency from a number of organizations. According to the DOJ, the group also allegedly created and deployed cryptojacking applications, and developed and fraudulently marketed a blockchain platform.

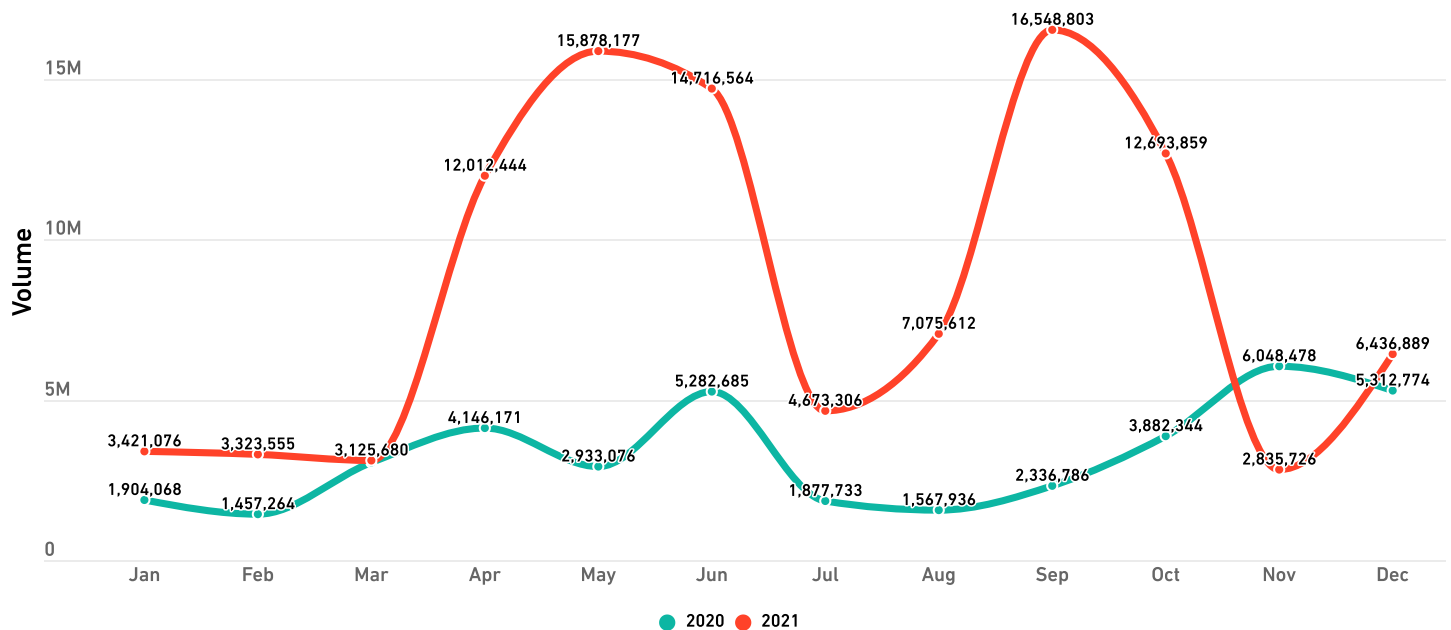
While you’d think these arrests would represent the final chapter of WannaCry, unfortunately this isn’t the case.

Microsoft issued a software patch for EternalBlue in March 2017, causing infections to plummet. *But WannaCry continues to this day:* In 2020, SonicWall observed 233,000 instances of WannaCry, and in 2021, there were 100,000 hits observed.

While these numbers are small compared with ransomware families such as Ryuk, by now the number of vulnerable Windows systems should be virtually zero. The fact that these infections are still numbering in the hundreds of thousands shows that, even five years on, there are *still* vulnerable Windows systems in the wild that need to be patched.

And the sooner, the better: WannaCry hits peaked in April 2021, when SonicWall Capture Labs threat researchers recorded 79,849 hits — evidence that coordinated WannaCry campaigns are *still* being run.

## Global Cerber Ransomware Volume







## 2021 Ransomware Trends

---

### Attackers' Horrifying New Tactic: Triple Extortion

In our mid-year report, we described the rising trend of [double extortion](#), a scam in which ransomware groups exfiltrate data prior to issuing a ransom note and encrypting the system, then use that data as leverage to increase the odds of securing payment.

But some organizations still refused to pay on principle, while others suspected — [with good reason](#) — that paying the ransom would not actually guarantee the safety of their data.

As ransomware operators recently discovered, however, just because an organization refuses to pay a ransom, that doesn't mean *its customers* will refuse to pay.

Like double extortion, triple extortion begins with ransomware operators exfiltrating large quantities of data, usually before encrypting the victim's network. But where double extortion groups threaten to release this data, triple extortionists filter through it, find out who might have the most to lose, and then demand ransom from them, too.

One of the first observed triple extortion cases highlights the ruthlessness of this scheme. In October 2020, an attacker calling himself "ransom\_man" [contacted Finnish psychotherapy provider Vastaamo](#). The attacker notified the provider that he possessed large quantities of Vastaamo's employee and patient data and demanded a ransom of 40 bitcoin.

While the company [reportedly paid the ransom](#), that wasn't enough for ransom\_man. Instead of deleting the stolen data,

the attacker began [contacting the therapy patients themselves](#), attempting to extort \$240 from them (\$500 if not paid within 24 hours) in exchange for not leaking their personal therapy session notes.

Even more shocking, however, is who the criminals targeted: The list of victims targeted included a number of children, [police officers and a dying man](#).

The REvil ransomware group is even adding such harassment to its RaaS offerings. In March, the group announced that it would, [as a free service](#), begin making voice-scrambled VOIP calls to notify the target's business partners and the media about the attack.

### Infrastructure Attacks

While ransomware attacks targeting infrastructure are [certainly nothing new](#), these attacks ramped up significantly in 2021.

Throughout the course of the year, just about every facet of everyday life was threatened by ransomware, such as [hospitals](#), [police departments](#), [water plants](#), the [fuel pipeline](#), [food producers](#) and [schools](#).

But while the payout for these sorts of attacks can be enormous, so can the press coverage and government scrutiny. Two ransomware groups — DarkSide and REvil — went into hiding following successful attacks. Much of the ransom collected from Colonial Pipeline by DarkSide [was seized by the Justice Department](#), and REvil [was arrested in early 2022](#).

## Notable Infrastructure Attacks in 2021:

### Colonial Pipeline – May 7, 2021

In May, cybercriminal group Darkside gained entry to America's largest fuel pipeline, Colonial Pipeline, via a compromised password posted on the Dark Web. In addition to enabling the [exfiltration of nearly 100 GB of data](#), the attack led to a six-day outage as the company investigated, causing fuel shortages, gas hoarding and panic. While Colonial reportedly paid the ransom to avoid release of the data, the group's gains were short lived. After the attack drew international attention, DarkSide [posted an apology](#) for "creating problems for society" and reportedly [disbanded](#) soon after.

### JBS Foods – May 30, 2021

The world's largest meat producer [was the victim of a ransomware attack](#) perpetrated by cybercriminal group REvil. This attack forced the company to temporarily close its beef plants in the U.S., disrupted a Canadian plant, and brought a halt to meat processing in Australia. While JBS claims that none of its data was exfiltrated, faced with the prospect of a prolonged shutdown, the [company admitted in June](#) that it had paid an \$11 million ransom.

## Cybercriminal group Darkside gained entry to America's largest fuel pipeline, Colonial Pipeline, via a compromised password posted on the Dark Web.

### NEW Cooperative – September 20, 2021

In September, ransomware group BlackMatter gained access to NEW Cooperative's network. The cybercriminal group reportedly [stole 1 TB of data](#) and threatened to release it if a \$5.9 million ransom was not paid. In the meantime, the company [lost access to the networks](#) used to accept grain shipments, deliver feed and keep feeding schedules on track for millions of chickens, hogs and cattle.

## Password Hygiene and MFA Could Have Stopped These Attacks

While these attacks were all devastating, they (along with 2020's SolarWinds attack) also share another commonality: They could have been prevented with better password hygiene and multi-factor authentication.

In late 2020, roughly 18,000 of SolarWinds' customers received SolarWinds software infected with malicious code. In a congressional investigation, it was revealed that [the use of the password "solarwinds123"](#) might have contributed to the breach.

In the case of JBS, a government investigation revealed that a weak password on an old administrator account [gave cybercriminals access to the network](#).

The Colonial Pipeline breach could almost certainly have been prevented with the use of two-factor authentication.

For NEW Cooperative, the reuse of a weak password — "chicken1" — on [at least 10 different accounts](#) across the company's 120 employees resulted in one of two outcomes: either an employee reused this password on an unrelated site that was breached and leaked to the Dark Web, or the use of brute-force attacks allowed the password to be easily guessed.

While cyberdefense has become more sophisticated and specialized over time, in some cases the simplest prevention is still some of the best.



## Phishing Goes Old School

Over the past several years, we've observed numerous phishing emails imitating correspondence from [Amazon](#) or [medical authorities](#). But in 2021, the FIN7 group, responsible for the BlackMatter and Darkside ransomware operations, decided to carry out a version of these campaigns [the old-fashioned way](#).

According to an FBI alert, starting in August, this group used UPS and USPS to snail-mail ransomware to U.S. businesses in the insurance, transportation and defense industries.

Targets received one of two packages: One, purportedly from Amazon, arrived in a gift box accompanied by a thank-you letter, a fake gift card and a USB drive. The other, disguised as a package from the U.S. Department of Health and Human Services, included a page of guidance regarding COVID-19 and a USB drive.

If plugged in, these drives — which are loaded with “BadUSB” attacks — [are able to register themselves as keyboards](#), emulate keystrokes, execute commands and install malware, ultimately creating an entry point for ransomware, commonly [BlackMatter or REvil](#).

## 2021's Biggest Busts

With the creation of the Department of Justice's Ransomware and Digital Extortion Task Force, and with a heightened focus on ransomware among government and law enforcement agencies around the world, 2021 boasted several major busts:

**Jan. 27** – In an attempt to disrupt NetWalker, a fast-growing Ransomware-as-a-Service (RaaS), authorities from the U.S. and Bulgaria confiscated \$454,000 in cryptocurrency, seized the group's Dark Web site and arrested Sebastien Vachon-Desjardins of Gatineau, Quebec.

**Feb. 17** – French and Ukrainian officials worked together to arrest several cybercriminals associated with the Egregor ransomware.

**June 4** – 55-year-old Alla Witte, otherwise known as Max, was arrested for her role in infecting millions of computers worldwide with Trickbot malware, often used in multi-stage ransomware attacks. According to the DOJ, Witte, a member of the Trickbot Group, reportedly worked as a malware developer and wrote code related to the control, deployment and payment of ransomware.

**June 7** – One month after the May 7 ransomware attack on Colonial Pipeline, the Department of Justice seized 63.7 bitcoins from ransomware group DarkSide. This amounted to most of the 75 bitcoin ransom paid by Colonial Pipeline.

**June 16** – With the help of Interpol, the Ukraine National Police arrested six members of the ClOp ransomware group, which employs double and triple extortion attacks and have allegedly cost victims in the U.S. and South Korea roughly half a billion dollars.

**Nov. 8** – In November, 22-year-old Ukrainian national Yaroslav Vasinskyi and 28-year-old Russian national Yevgeniy Polyanin were arrested. Vasinskyi is allegedly responsible for the July 2 Kaseya ransomware attack, and Polyanin had conducted numerous Sodinokibi/REvil ransomware attacks, scamming millions from his victims. \$6.1 million in ransom payments was also seized during this arrest.



# Cryptojacking



## Bigger than Ever

In 2021, the number of cryptojacking attempts rose to 97 million, an increase of 19% year over year and an average of 338 cryptojacking attempts per customer network.

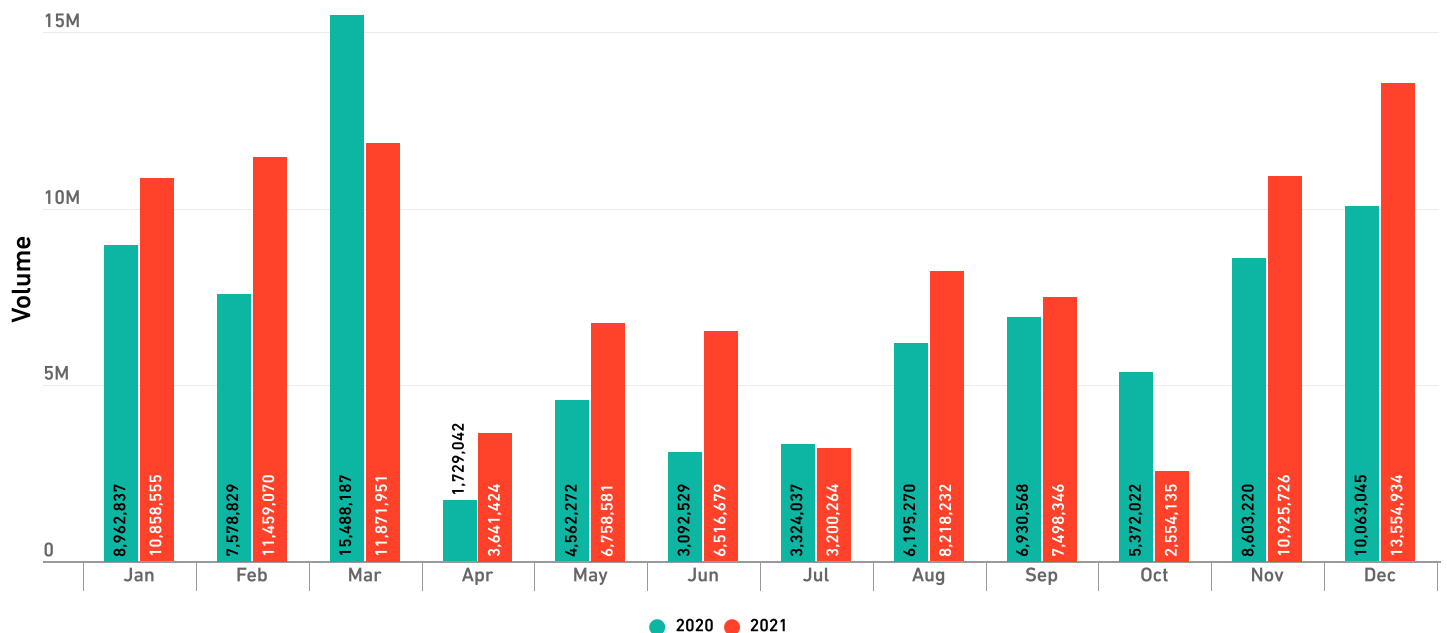
While cryptojacking volume didn't see the sort of triple-digit increases that were observed with ransomware and encrypted attacks, this moderate increase was still enough for 2021 to set a new all-time record.

This wasn't the only cryptojacking record 2021 set, however. With 34.2 million hits, the first quarter of 2021 saw more cryptojacking than any other quarter since SonicWall began tracking it.

But worryingly, the worst month for cryptojacking in 2021 was, by far, December: While the 13.6 million hits recorded in December don't eclipse the anomalous 15.5 million hits observed in March 2020, it makes for an easy second place, and a highly suboptimal starting point for 2022.

**With 34.2 million hits, the first quarter of 2021 saw more cryptojacking than any other quarter since SonicWall began tracking it.**

## Global Cryptojacking Volume



"How to Deal with Business Email Compromise," Osterman Research, Sponsored by SonicWall, January 2022



# Cryptojacking by Region

Despite 2021 being a record-breaking year, only one region saw a large increase: Europe, where cryptojacking volume rose 60% according to SonicWall data.

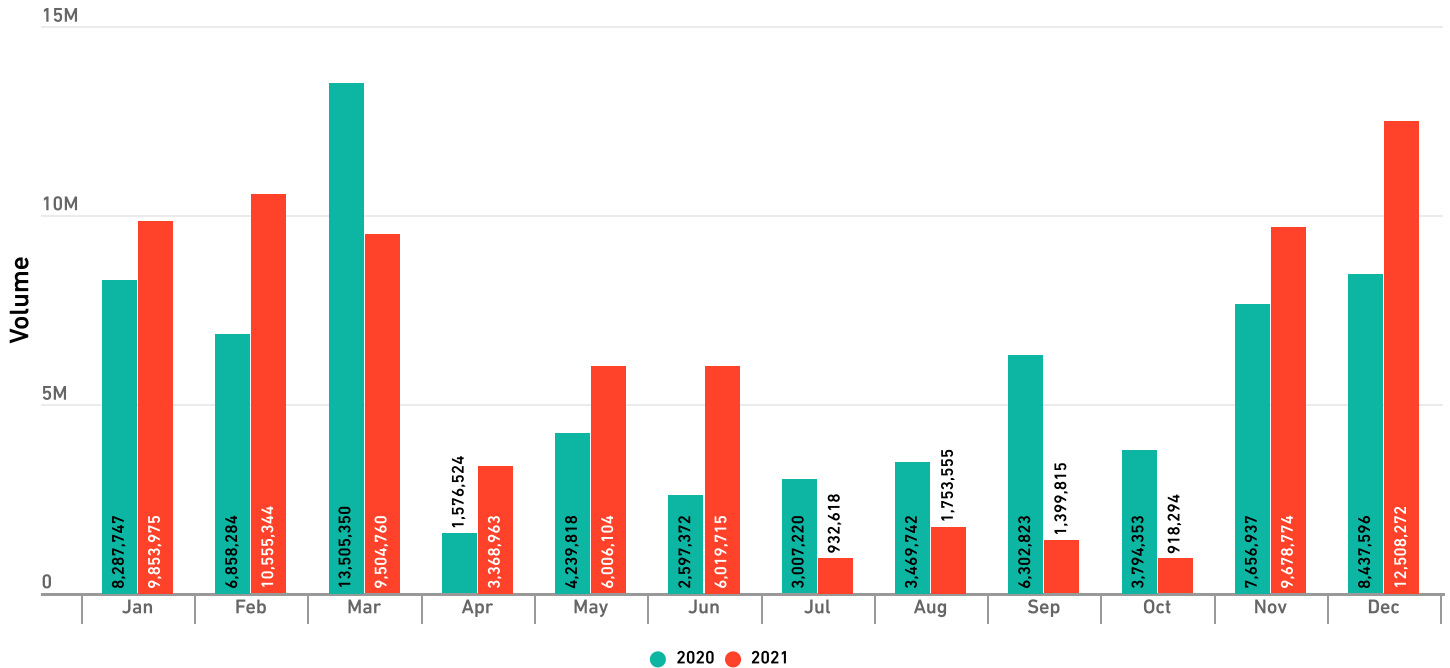
North America saw a year-over-year rise in cryptojacking as well, but at 13% it was fairly modest — especially compared to the 260% jump recorded in 2020.

In Asia, cryptojacking continued the massive freefall that began in 2019. While cryptojacking that year reached 35.7 million hits, volume fell 87% in 2020 and another 37% in 2021. Asia’s cryptojacking volume in 2021 was just under 3 million hits — less than a tenth of what it was two years ago.

## North America saw a year-over-year rise in cryptojacking

In the U.S., cryptojacking volume rose just 4%, due in part to a highly depressed Q3. In contrast with Q1 and Q4, which notched 30 million hits and 23.1 million hits respectively, the entirety of Q3 saw just 4.1 million hits — or 5.7% of the total yearly cryptojacking volume.

### Cryptojacking Volume | United States



# Cryptojacking by Industry

A number of industries also showed aggressive year-over-year growth in cryptojacking volume. For government and healthcare customers, this increase was in the triple digits, with cryptojacking growing 709% and 218% respectively.

Despite these increases, education customers are the ones most likely to see a cryptojacking attack. This is the second year in a row for which this is held true, but fortunately for education customers, the average percentage per month who saw an attack appears to be dropping.

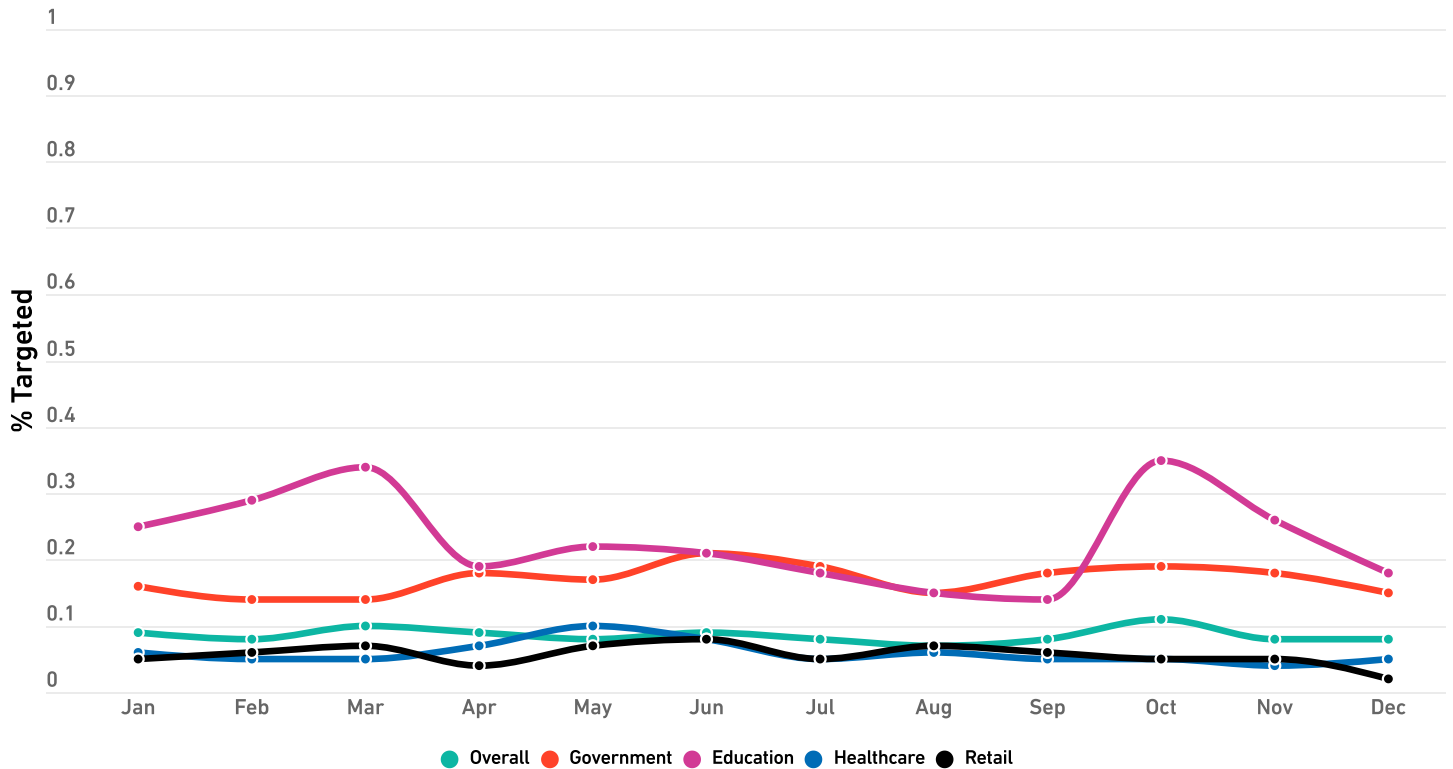
## How Cryptojacking is Spreading

In years past, cryptojacking spread primarily through fileless malware, phishing attempts with malicious links, malvertising and more. Some cryptojacking scripts have even been designed with wormlike abilities, allowing them to spread across networks.

**For government and healthcare customers, this increase was in the triple digits, with cryptojacking growing 709% and 218% respectively.**

In 2021, SonicWall Capture Labs threat researchers also observed cryptojacking spreading via pirated/ cracked software, public project hosting websites and vulnerable web servers.

**% of Customers Targeted by Cryptojacking in 2021**



In the latter case, SonicWall Capture Labs threat researchers in November observed malware [targeting the Alibaba Cloud \(Aliyun\) cloud computing program](#) — the fourth-largest cloud provider globally behind Amazon Web Services, Microsoft Azure and Google Cloud.

After disabling Alibaba’s cloud monitoring agent and cloud assistant service, the malware is able to execute without notifying the machine’s owner. It disables other processes and cryptomining services that can compete for CPU resources, then downloads and executes the XMRig miner.

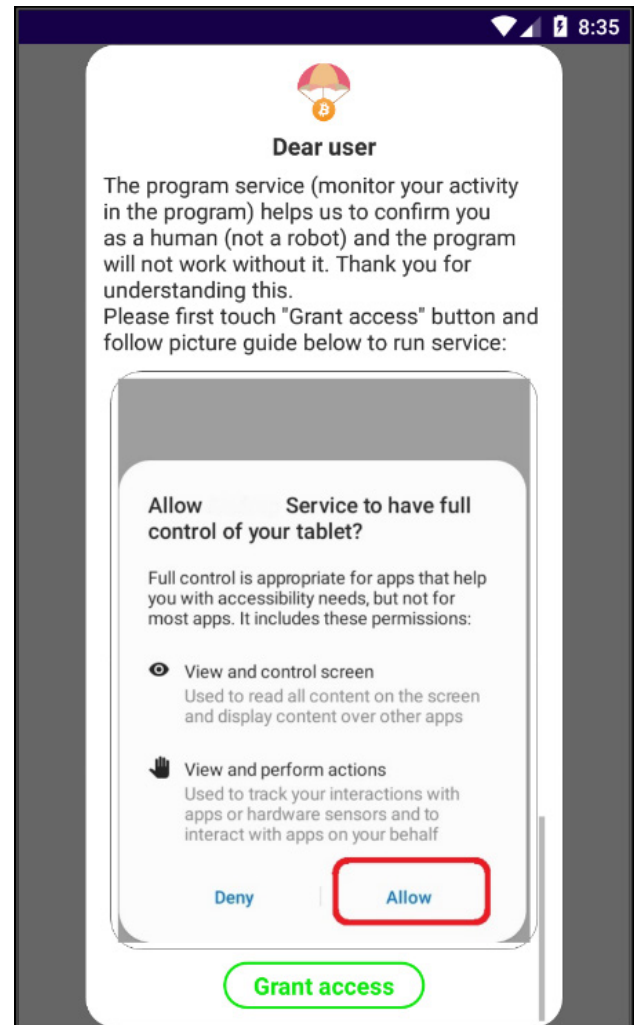
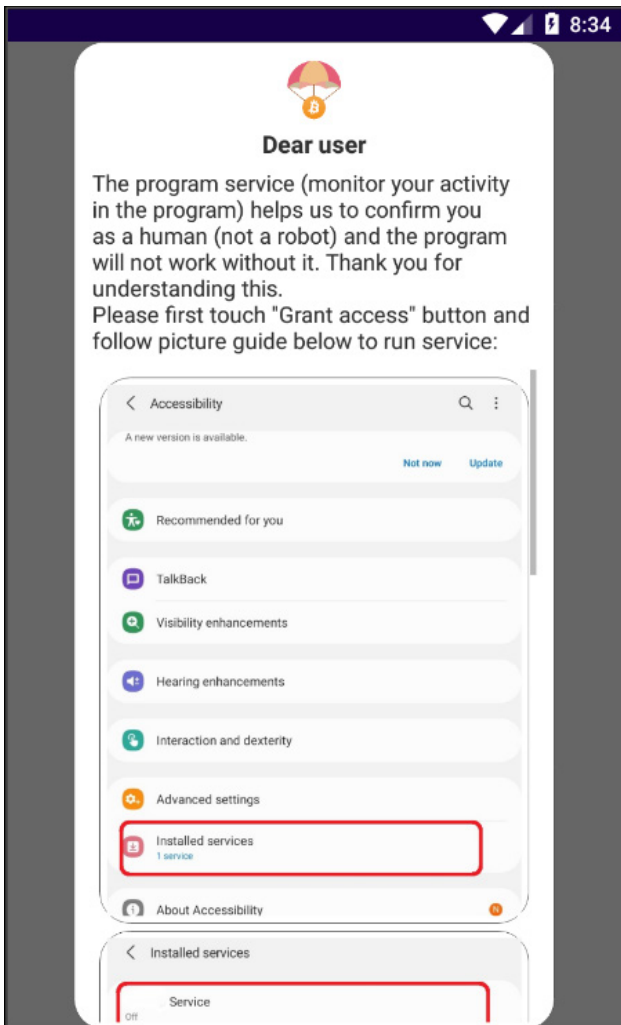
Due to being widely available and easy to use, XMRig continued to be the cryptojacking program of choice in 2021. One of the file-based cryptojacking tools that came to prominence following Coinhive’s shuttering in 2019, XMRig is an open-source cross-platform miner.


It’s dropped on the victim’s machine by a number of different types of malware, such as Vivin and BlueMockingbird, or the [self-spreading Golang-based malware](#).

### The Rise of Cryptocurrency Stealers

Cybercriminals are always on the hunt for a quicker and easier way to make money. So, when it became possible to steal cryptocurrency from a machine directly, instead of making the machine mine coin over time, attackers jumped on board.

In November, SonicWall Capture Labs threat researchers [identified an Android app](#) (see below) designed to steal crypto wallets from victims. This malicious app is called “Trust: Crypto & Bitcoin Wallet,” and purports to be associated with the (legitimate) TrustWallet cryptocurrency wallet.





But despite its name, it isn't to be trusted: Once installed, the malicious app requests the user grant Accessibility Services "to confirm you as a human (not a robot)," and notifies the user that the app will not work without these services being turned on. Once on, this app can perform clicks in the background without the user's knowledge and, by acting on behalf of the user, it automatically transfers the cryptocurrency from the user's wallet to the wallet of the malware operator.

Criminals don't always go after individuals' crypto wallets, however. Sometimes they attack cryptocurrency exchanges directly. In 2021, there were [over 20 attacks on crypto exchanges or projects](#) in which a cybercriminal stole at least \$10 million in cryptocurrencies. And in more than a quarter of these cases, the amount stolen surpassed the \$100 million mark.

In August, the Poly Network was breached when an attacker "[exploited a vulnerability between contract calls](#)," and stole a reported \$610 million (all of which was [ultimately returned](#).)

And in December, armed with [a stolen private key](#), attackers stole a reported \$200 million in cryptocurrency from trading

---

**In 2021, there were over 20 attacks on crypto exchanges or projects in which a cybercriminal stole at least \$10 million in cryptocurrencies. And in more than a quarter of these cases, the amount stolen surpassed the \$100 million mark.**

---

platform BitMart. (Ironically, most of the digital currency stolen [was SafeMoon](#).) While the platform has vowed to return the stolen coin with its own funds, more than a month later some users [were still waiting](#) to get their money back.

## The True Cost of Crypto Continues to Mount

---

Long gone are the days when anyone with a decent rig can mine cryptocurrency and expect to make a healthy profit. Today's mining is complex enough that even those with top-tier PCs and high-end GPUs have trouble mining enough to really make it worth their while.

One of the "benefits" of cryptojacking, however, is that the costs are all borne by someone else, while the attacker reaps all the benefit.

And increasingly, "someone else" means "everyone else." According to a study by [The New York Times](#), the process of creating bitcoin requires a whopping 91 terawatt-hours of electricity each year — more than is used by the entire nation of Finland and more than [is used by Google, Facebook, Apple and Microsoft combined](#).

From 2015 to 2021, the amount of energy used to mine Bitcoin alone [increased almost 62-fold](#), and now amounts to nearly half a percent of the electricity consumption of the entire world.

# Encrypted Attacks

## Encrypted Attacks Show Triple-Digit Increase

2021 was among the most turbulent years on record for many threat trends, but the movement of encrypted attacks was wild even by those standards. Year over year, malware sent over HTTPs rose 167% — and on their way up, they set several new records.

All told, SonicWall recorded 10.1 million encrypted attacks in 2021, almost as many as 2018, 2019 and 2020 put together. This meteoric increase was driven by triple-digit increases in North America, Europe, and Asia, where attack volume rose 220%, 142% and 201% respectively. Not a single region showed a decrease in 2021.

While you wouldn't expect a year with triple-digit growth to include an all-time low, January 2021's encrypted attack volume was just that. Attacks then doubled in February, and then doubled again in March. But despite all this doubling, the first half of the year only represented about 20% of the number of encrypted attacks we would see in 2021.

When the second half of the year arrived, it immediately brought a record of its own. A total of 864,206 encrypted attacks were recorded in July, narrowly edging out the previous record high of 811,144, set in August 2020.

But while August 2020's spike would prove to be a blip, August 2021's spike was anything but. That month saw attack volume surpass 1 million for the first time, and for the remainder of the year, only one month (October) would see attack volume dip below 1 million.

December would bring yet another record, one that would blow all previous totals away. From Dec. 1 to year's end, SonicWall Capture Labs threat researchers recorded a staggering *2.5 million encrypted attacks* — more than 25 times the number of encrypted attacks recorded in the month of January.

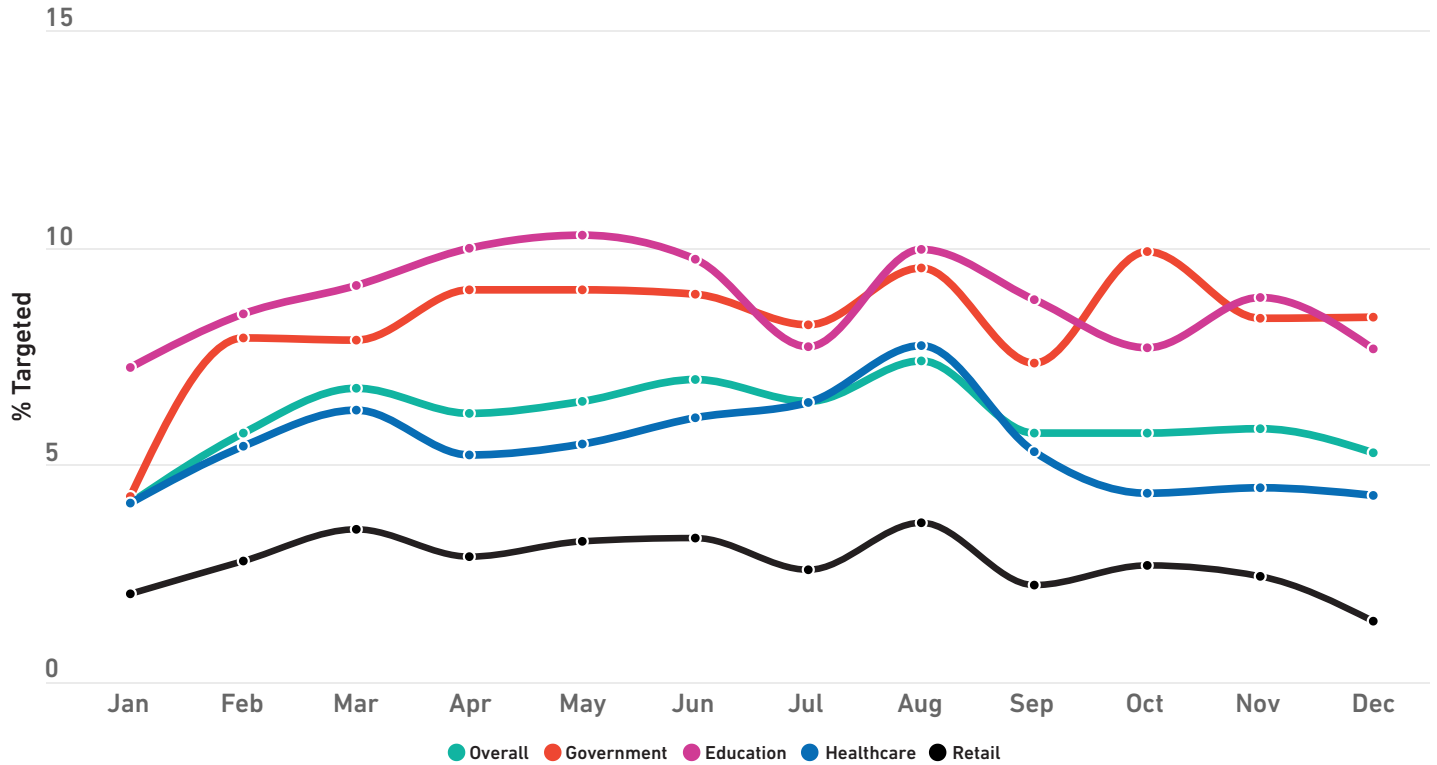


## Encrypted Attacks by Industry

The education sector faced a deluge of attacks in 2021, but it wasn't the only one. An average of 8.8% of education customers saw an encrypted attack in a given month, compared with 8.2% of government customers. Retail customers, on the other hand, were comparatively spared: An average of just 2.7% of customers saw an attack per month.

While monthly trends were all over the place, two commonalities held across industries: The percentage of customers who saw an attack was at its lowest in January, and all industries saw a large spike in August that disappeared about as quickly as it came.

### % of Customers Targeted by Malware over HTTPS in 2021



## What Are Encrypted Threats?

In simple terms, TLS (Transport Layer Security) is used to create an encrypted tunnel for securing data over an internet connection. While TLS provides legitimate security benefits for web sessions and internet communications, cybercriminals increasingly use this encryption protocol to hide malware, ransomware, zero-day attacks and more.

Traditional security controls, such as legacy firewalls, lack the capability or processing power to detect, inspect and mitigate cyberattacks sent via HTTPS traffic, making this a highly successful avenue for hackers to deploy and execute malware.

# Intrusion Attempts

## Malicious Intrusion Attempts Fall By Nearly a Third

In 2021, SonicWall Capture Labs threat researchers recorded 5.28 trillion intrusion attempts — a 10.7% increase over the number of attacks in 2020, and roughly five times as many attempts as there were in 2013, the first year SonicWall reported this data.

But it's important to note that these 5.28 trillion intrusion attempts represent a combination of three severity types: low, moderate and high. Low-severity hits typically consist of things like scanners and pings — actions which are not malicious and pose no threat to the target.

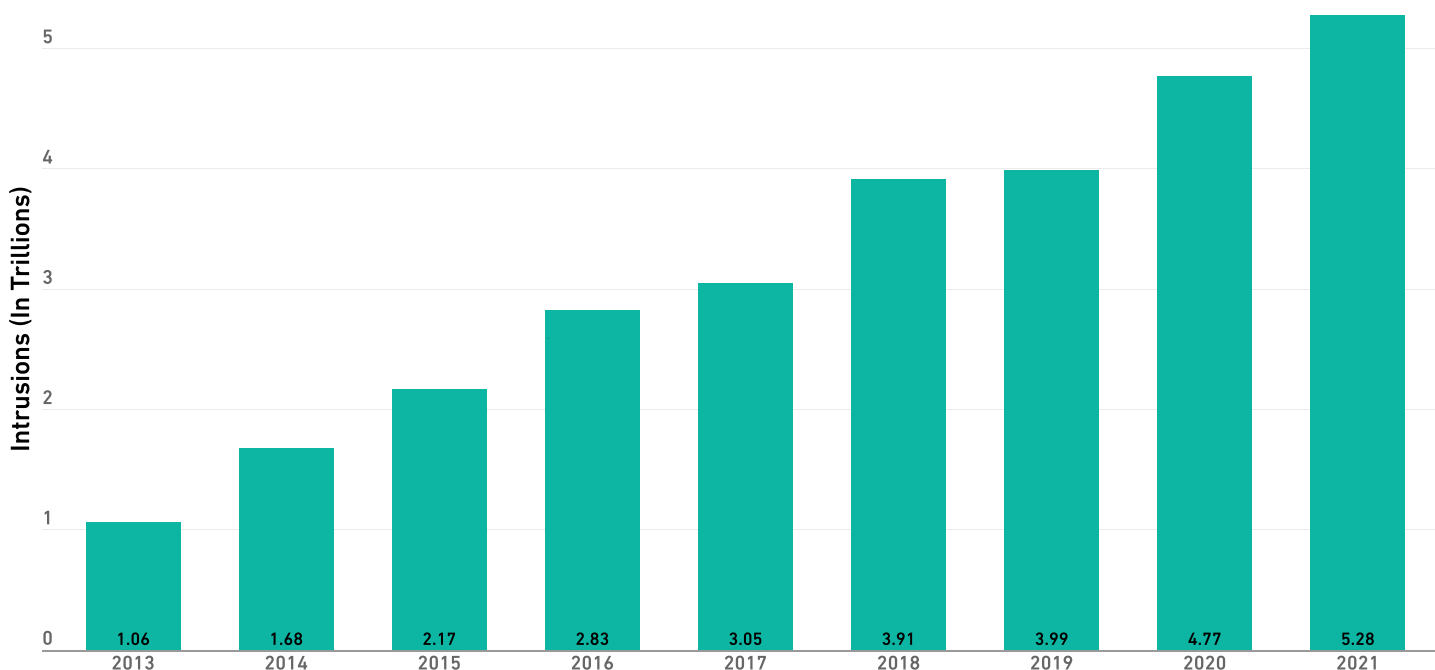
If we isolate the moderate and high severity intrusion attempts — also called malicious intrusion attempts — we find much better news. In 2021, the volume of these attacks fell by 28% year over year.

2021 also ended the run of months with intrusion attempts over 1 billion. This streak began in March 2020, when attempts abruptly jumped from 777 million to 1.05 billion. Once this milestone was passed, intrusion attempts remained above 1 billion for the rest of the year.

At the beginning of 2021, this pattern was still going strong. But in April, intrusion attempts dropped like a rock, falling from 1.5 billion to 874 million. Once intrusion attempts fell below 1 billion in 2021, they stayed there for the rest of the year.

This decrease contributed to a top-heavy year: The first half of 2021 had over 2 billion more malicious intrusion attempts than the second half, a much more positive trend we hope will persist into 2022.

### Global Intrusion Attempts



## What is an Intrusion Attempt?

A malicious intrusion attempt is a security event in which an intruder, hacker, cybercriminal or threat actor attempts to gain access to a system or resource by exploiting a vulnerability without authorization. These vulnerabilities are typically public and published as CVEs, discussed in a previous section. While the vulnerability is public, not everyone patches at the same rate, and attacks take advantage of unpatched appliances or software that can be used as an entry into a network. (A more serious and dangerous scenario is when a vulnerability is not yet well publicized or has not yet been published — these are the dreaded zero-day vulnerabilities.)

Exploitation of vulnerabilities does not stop once the attackers get inside the network. Instead, that's when they pick up the pace: Attackers will gain lateral movement and network persistence by exploiting other, internal vulnerabilities in unpatched systems and software once inside the network.

What SonicWall records is detection and prevention of vulnerabilities — coming both from external and internal sources. When a piece of code that constitutes a vulnerability passes a firewall with Intrusion Prevention enabled, and the firewall detects and neutralizes that code, an intrusion attempt is counted.

As noted, low-severity intrusions are typically benign.

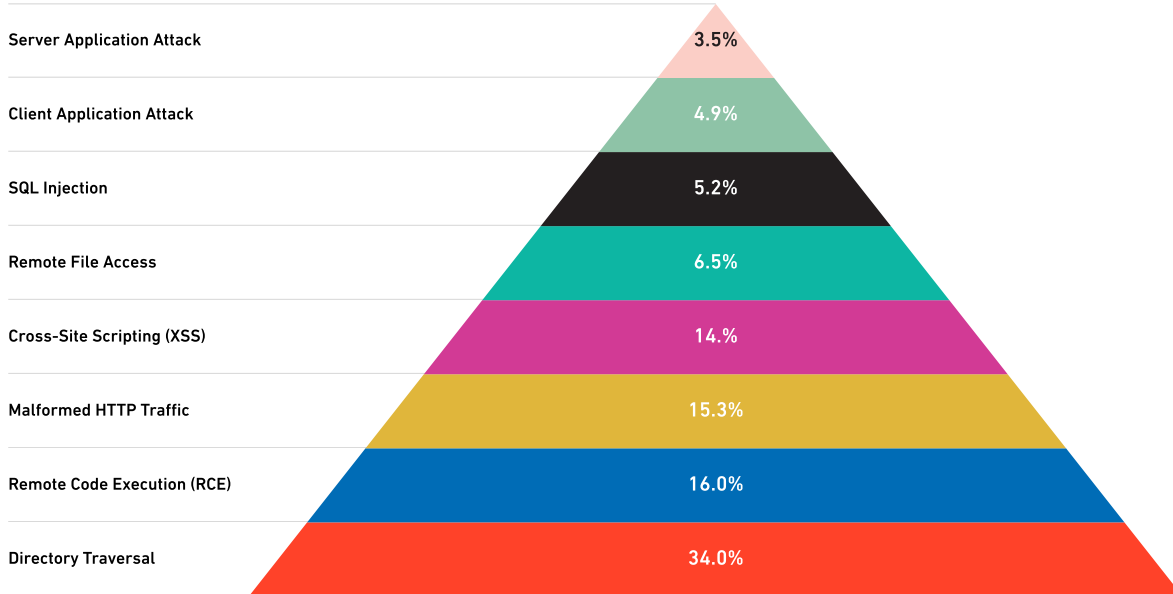
## Malicious Intrusions by Type

There's been a lot of movement in the different sorts of intrusion attempts over the past few years. In 2019, Remote Code Executions, or RCEs, were the top form of malicious intrusions, but that shifted to Directory Traversal in 2020. In 2021, Remote File Access attempts moved to the top.

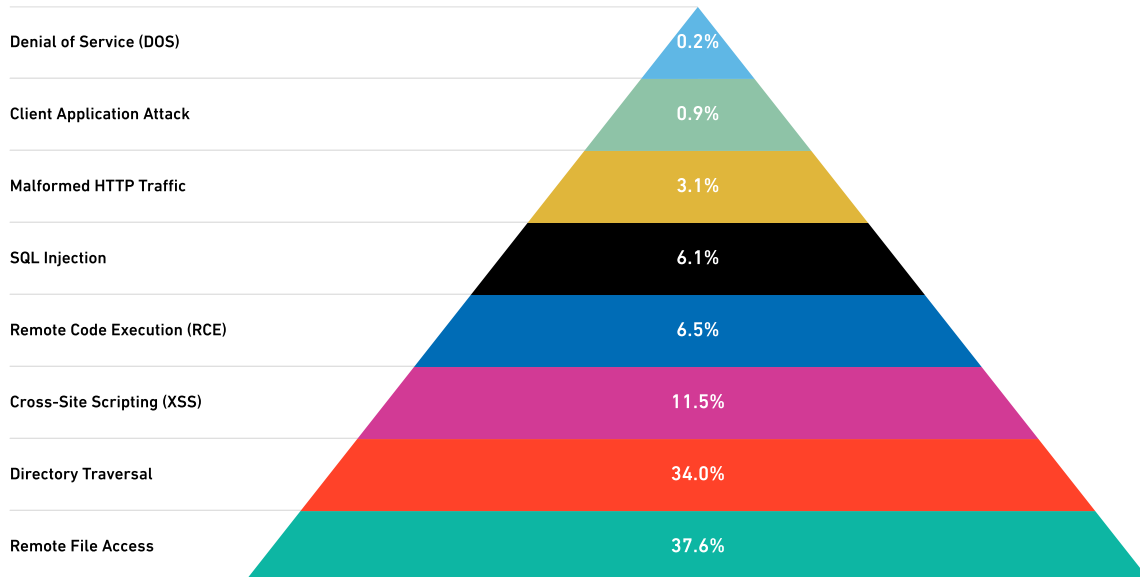
## Malicious Intrusions by Region

When malicious intrusion attempts dropped, they dropped across the board. But there was a wide variety in the amount of decrease. Europe showed the greatest drop, with attempts falling 50% year over year. In Asia, attempts fell by 17%, and in North America — where more than half of 2021's intrusion attempts occurred — attempts fell by only 2%.

### 2020 Malicious Intrusions



### 2021 Malicious Intrusions





# Top Intrusion Attacks

---

## Remote File Access

Remote file access refers to an unauthorized individual gaining access to a file meant to be accessed by authorized individuals only.

## Directory Traversal

Also known as a path traversal attack, a directory traversal attack is an exploit that aims to access files and directories that are not located under the “working” directory. This is done by manipulating file variables, so that characters representing “traverse to parent directory” are passed through to the operating system’s file system API. This allows attackers to obtain sensitive files not intended to be seen outside the appliance or software.

## Cross-Site Scripting (XSS)

XSS attacks are client-side code injection attacks that insert malicious code, most commonly JavaScript, into the script of legitimate applications or websites. When a user visits these hacked pages or apps, the malicious code is executed, sending the malicious script to the victim’s browser, with the ultimate goal of stealing the victim’s information.

## Remote Code Execution (RCE)

An RCE attack takes place when a cybercriminal uses a vulnerability to remotely run malicious programming code, usually in an unexpected path and with system-level privileges. The Bluekeep vulnerability is an example of this. These vulnerabilities are among the most dangerous on software systems and are frequently used to spread ransomware.

## SQL Injection

SQL injections occur when malicious SQL statements are injected into vulnerable applications or websites. This allows attackers to manipulate backend databases and retrieve or alter database information that was not meant to be accessible, in some cases giving the attacker complete control over your database. Since databases can also control access (i.e., user names and passwords), SQL injection attacks can lead to credential theft, which can then lead to unauthorized access.

## Malformed HTTP Traffic

Malformed HTTP traffic consists of patterns not seen in legitimate HTTP requests or responses — for example, oversized HTTP headers.

## Client-Application Attack

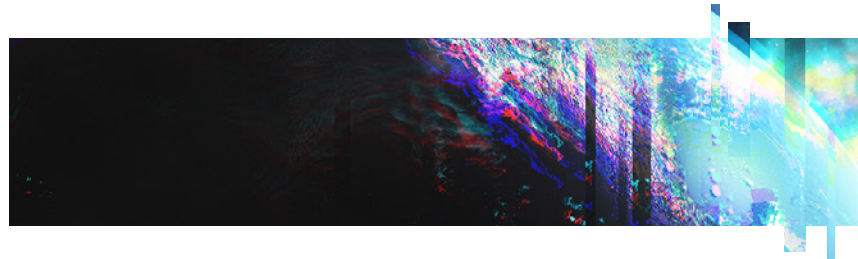
Client-application attacks occur when attackers target client applications directly — for example, memory leaks.

## Denial of Service

A denial-of-service (DOS) attack, or sometimes a distributed denial-of-service (DDoS) attack, is an attempt to make an online service unavailable by overwhelming it with heavy amounts of traffic, making it impossible for legitimate users to access the site or service. In the DDoS scenario, which is more common, the traffic is launched from multiple sources to avoid easy detection and prevention. In many cases, especially with DDoS attacks, large malicious botnets are often leveraged to flood a target site, system or application until it is inaccessible or inoperable. Mirai was one of the most famous DDoS attacks, which targeted many global DNS services and brought much of the internet down in late 2016.



# Capture ATP & RTDMI



## RTDMI Gets Smarter, Faster, Better

2021 was another banner year for SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) technology. A total of 442,151 total never-before-seen malware variants was identified in 2021, a 65% increase over 2020's count and an average of 1,211 per day.

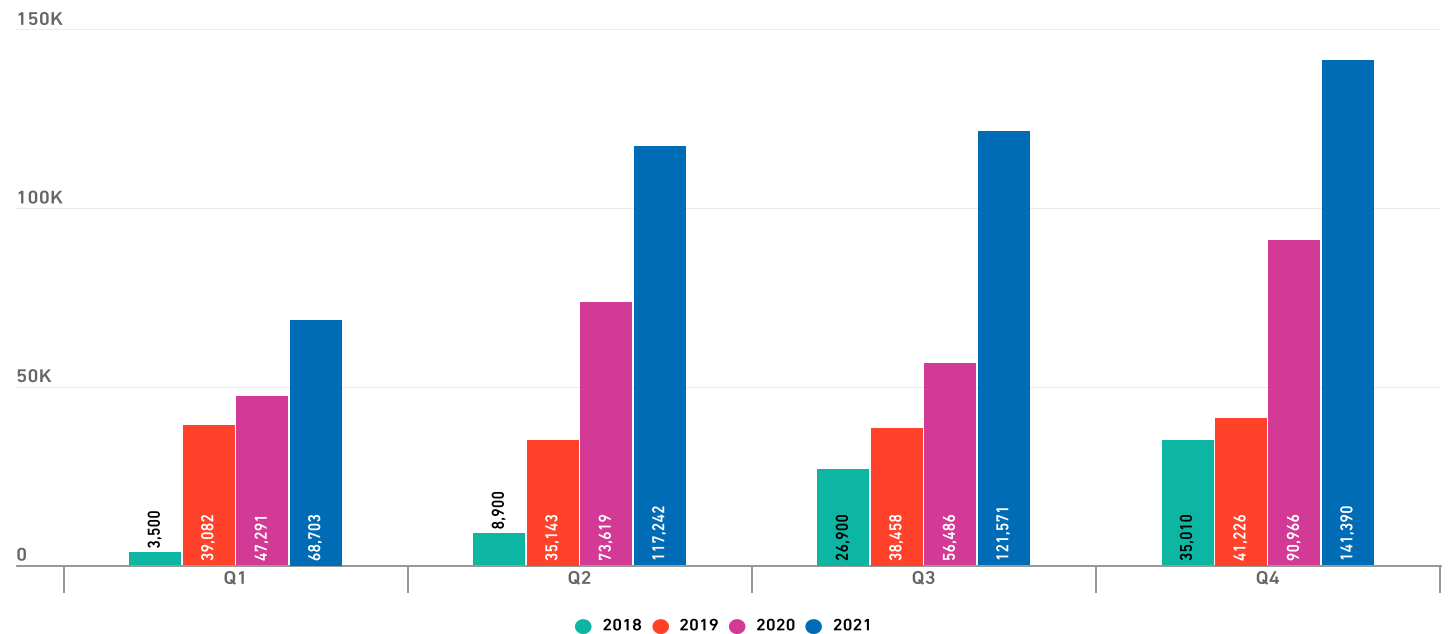
When RTDMI was added to SonicWall's existing Capture Advanced Threat Protection, it began identifying a large number of never-before-seen malware variants almost immediately. RTDMI is capable of finding malware that relies on various anti-evasion techniques — frequently variants of existing malware that have been obfuscated, repacked or recompiled in such a way as to evade all existing industry detections.

## What Is RTDMI?

Introduced in early 2018, SonicWall's patented Real-Time Deep Memory Inspection™ engine detects and blocks malware that doesn't exhibit malicious behavior and hides its weaponry via encryption.

Each year, RTDMI leverages proprietary memory inspection, CPU instruction tracking and machine learning capabilities to become smarter, more agile and more efficient at recognizing and mitigating cyberattacks never before seen by anyone in the cybersecurity industry.

'Never-Before-Seen' Malware Variants Found by RTDMI™





This growth has produced a number of new milestones. In October 2021, the monthly total of never-before-seen variants reached 50,418, surpassing the 50,000 mark for the first time ever. This feat would be repeated the very next month, when the total for November reached 51,633.

In 14 of the last 16 quarters, the number of new malware variants has exceeded that found in the previous quarter. A total of 141,390 never-before-seen malware variants were recorded in Q4 2021 — more than any quarter on record.

This growth indicates that the creation of new variants for existing malware — ones able to bypass detection by a majority of the industry tools on the market — is becoming increasingly accessible and more frequently utilized. This is a worrisome development: If any one of these attacks gets past an organization’s defenses, it can result in a ransomware infection.

### A Year of 100% Detection — And (Still) No False Positives

While our internal data is a testament to the power of RTDMI, its capabilities have also been proven by third-party testing — not just once, but four times in a row.

ICSA Labs Advanced Threat Defense (ATD) testing evaluates vendor solutions designed to identify new threats that other traditional security products do not detect, and focus on how

effectively solutions detect these unknown and little-known threats while minimizing false positives.

It’s rare enough for any vendor to score 100% with no false positives. No vendor had ever earned this score twice in a row — let alone four times in a row.

### 2021 ICSA ATD Testing Cycles

QTR	MALICIOUS SAMPLES DETECTED	BENIGN SAMPLES DETECTED	MALICIOUS DETECTION RATE	FALSE POSITIVE RATE
Q1	580/580	0/891	100%	0%
Q2	544/544	0/600	100%	0%
Q3	653/653	0/695	100%	0%
Q4	801/801	0/824	100%	0%

“Armed with more than a decade of machine-learning experience, RTDMI plays an essential role in quickly identifying destructive malware strands not detected by traditional sandboxing technology,” said SonicWall SVP and Chief Technology Officer John Gmuender. “As cyberattacks continue to strengthen and escalate, so must technology and the creative thinking of researchers who work around the clock to ensure that organizations in all industries can advance their reliance on the digital and connected world.”

## “Zero-Day” vs. “Never-Before-Seen” Attacks

The “zero-day attack” is among the most well-known cybersecurity terms due to its connection to high-profile breaches. These attacks are completely new and unknown threats that target a zero-day vulnerability without any existing protections (such as patches, updates, etc.) from the target vendor or company.

Conversely, SonicWall tracks detection and mitigation of “never before seen attacks”, which are the first time SonicWall Capture ATP identifies a signature/SHA256 as malicious. These discoveries often closely align with zero-day attack patterns due to the volume of attacks analyzed by SonicWall.

# Malicious PDF/Office Files



## Malicious Office and PDF Files Reverse Course

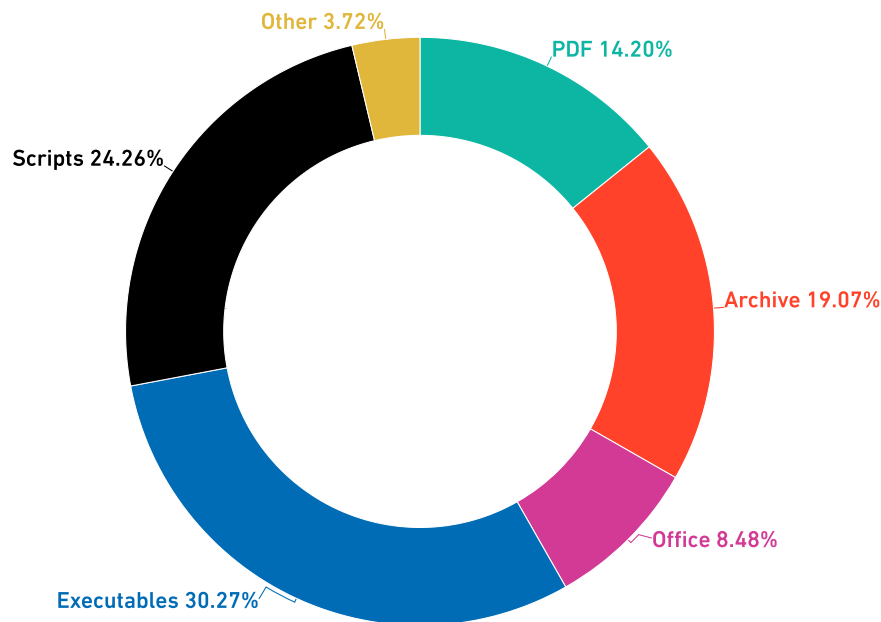
In 2021, SonicWall Capture Labs threat researchers recorded a 52% year-over-year increase in the overall use of malicious PDFs, while use of malicious Microsoft Office files fell 64%.

This represents a significant reversal from a year ago. In 2020, SonicWall Capture Labs threat researchers noted that cybercriminal groups were shifting from PDFs to Office files in their 2021 malware campaigns, driving last year's percentage of malicious PDF files down 22%, and catapulting the percentage of malicious Office files up 67%.

But it's important not to conflate the *percentage increase* with the *percentage of total files*. For instance, the number of malicious PDFs detected showed double-digit growth, but since PDFs only represented 9.2% of all malicious files last year, the percentage of total malicious files that were PDFs was still pretty small in 2021.

**SonicWall Capture Labs threat researchers noted that cybercriminal groups were shifting from PDFs to Office files in their 2021 malware campaigns.**

## 2021 New Malicious File Type Detections | Capture ATP





Office files, on the other hand, were a quarter of all malicious files identified, but this year represent less than 1 in 10. .Exe files picked up most of the slack, doubling from just over 15% to roughly 30%.

### Beware Muscle Memory

With cloud platforms overtaking programs installed on devices, and with two-factor authentication (2FA) becoming the norm among companies looking to harden their security posture, the average user now enters their login credentials several times a day. While it's tempting to let muscle memory take over and get through the process as quickly as possible, doing so may open you up to credential theft.

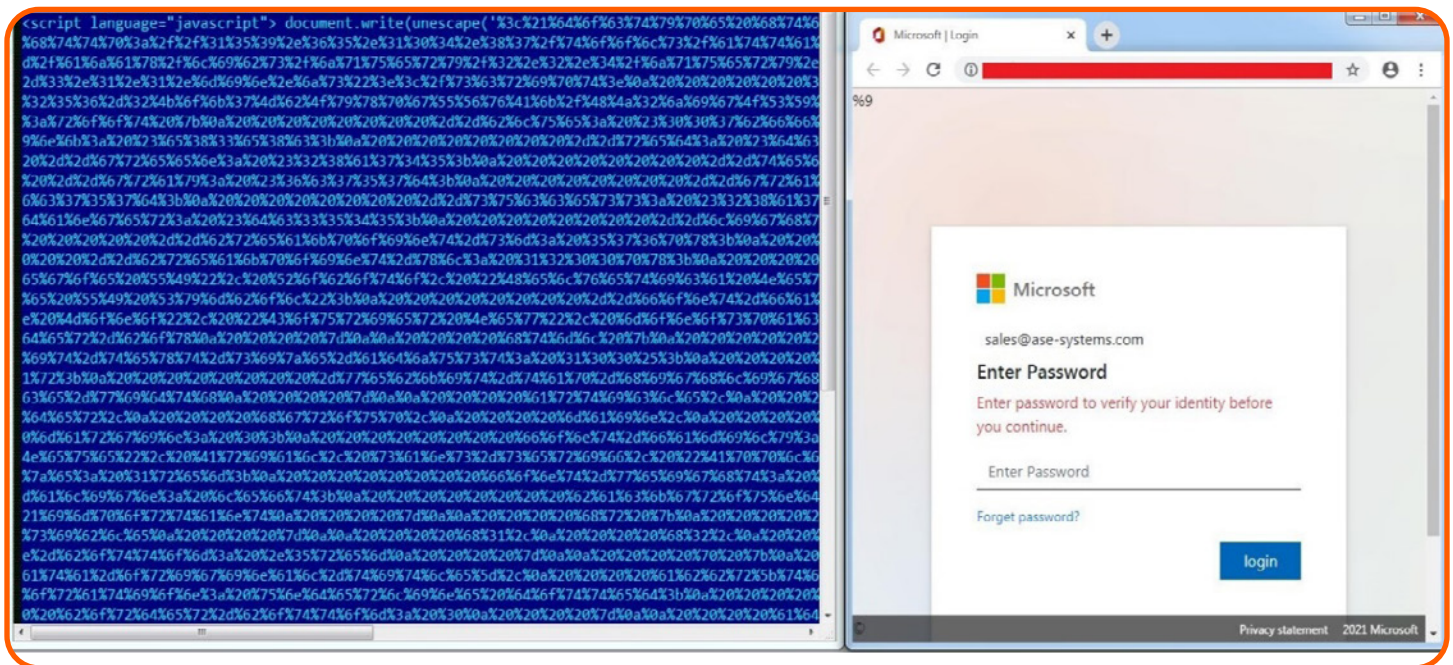
In 2021, SonicWall identified several phishing campaigns designed to trick busy or distracted employees.

A majority of the HTML phishing emails observed in 2021 were designed to launch a login form, which is prefilled with a user's email address. All you have to do is enter your password —cybercriminals are counting on well-practiced users to do this in about two seconds, not long enough to notice that anything might be amiss.

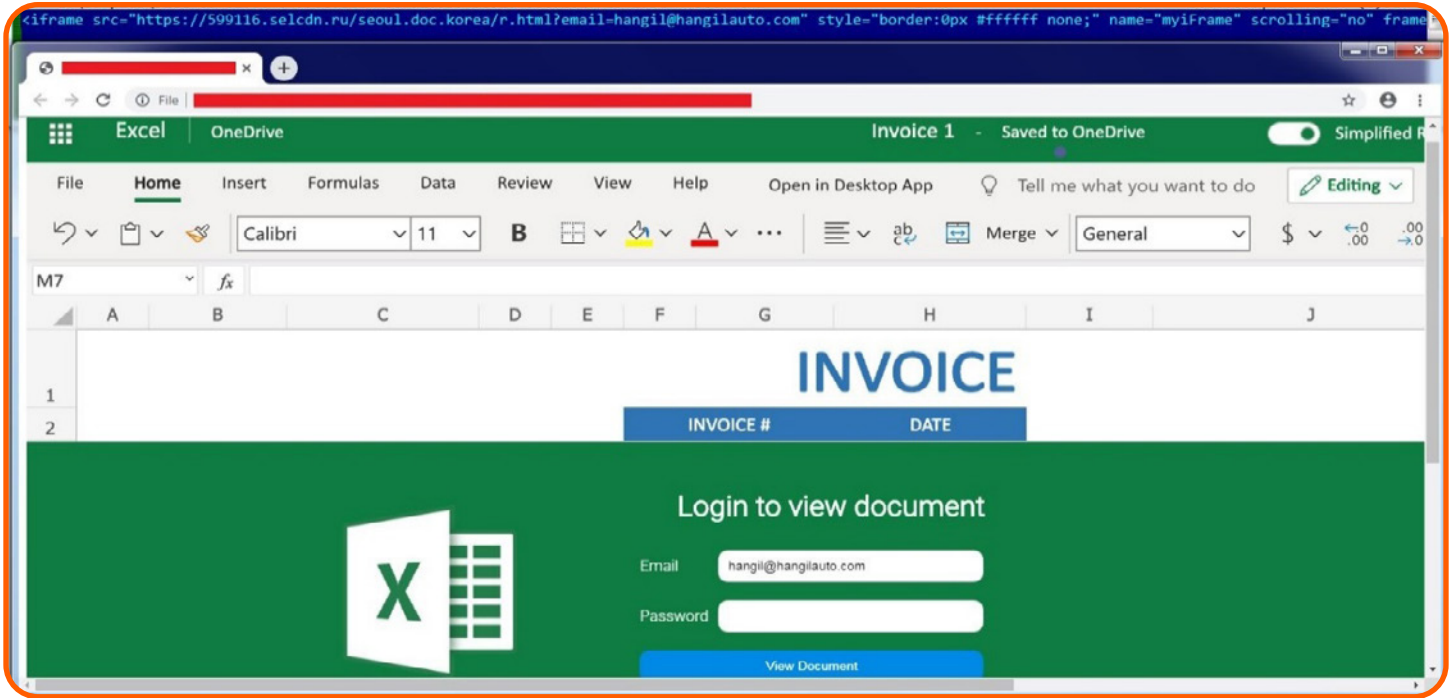
## A majority of the HTML phishing emails observed in 2021 were designed to launch a login form, which is prefilled with a user's email address.

Once the user enters their password, it's sent to the malware-hosted remote server and the user is redirected to some legitimate website.

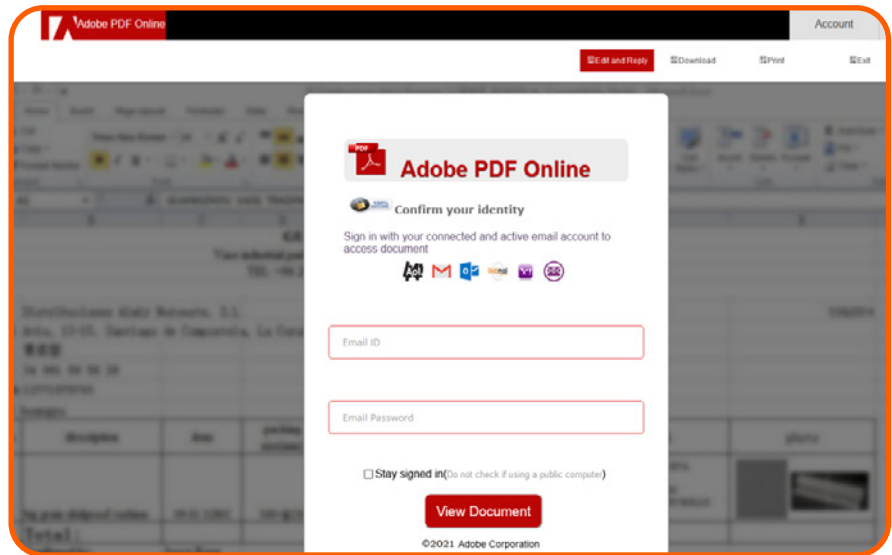
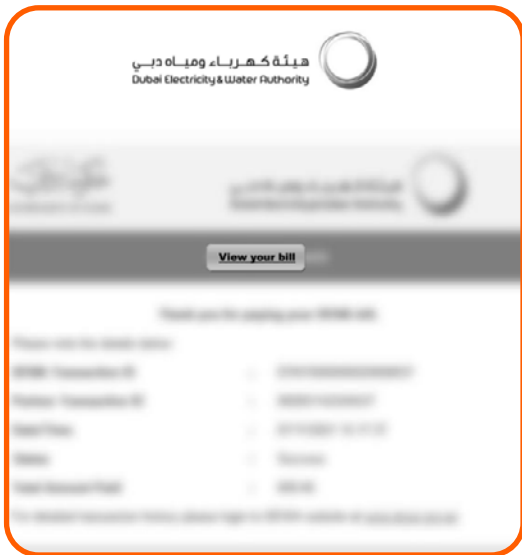
This trend of using “authentication fatigue” to harvest credentials has also been observed in phishing campaigns using PDF files. While most attempt to steal Microsoft Office credentials, researchers encountered files attempting to steal Dropbox, Amazon, DHL, Google Drive and Adobe credentials as well.



The embedded JavaScript on the left displays the legitimate-looking login form on the right.



In this case, the iframe asks for the user’s password, with the word “invoice” visible to boost legitimacy and increase urgency.



In this highly targeted example, the PDF is designed to imitate a Dubai Electricity and Water Authority bill. The image is blurred, but there is a link reading “View your bill” that, when clicked on, leads to a phony Adobe login page.

## Filenames to Look Out For in 2022

The trend of borrowed legitimacy continued to the filenames used in these campaigns. Because most people know enough to look at a filename before opening it — and because virtually no one is going to open a file with a name like “InfoStealer.xlsm” or “malware.exe” — phishing groups name their malicious files to maximize both gravitas and urgency.

But while you’re highly likely to receive a malicious file called “Document,” the odds of it actually being a document (as in, a Microsoft Word file) are only about 1 in 12. The vast majority of malicious Office files are Excel spreadsheets, with .xlsm being the most common extension.

## 2021's Top 10 Malicious Office File Names:

FILENAME BEGINS WITH	SHARE OF MALICIOUS FILES
Document	33.84%
Rebate	6.82%
Complaint	5.52%
Debt	4.48%
Permission	2.43%
Compensatio72021.xlsm	2.26%
Cancellatio242021.xls	1.90%
Overdue	1.76%
Outstanding42021.xlsm	1.70%
Claim	1.62%

## Who is Rabota?

Along with the trends and volume associated with malicious Microsoft Office files, SonicWall also tracks various other attributes of these files. In 2021, researchers noted that there was a roughly 50% chance that, if you came across a malicious Office file, it would have “Rabota” listed as the author.

While this sounds like it could be someone’s name, there isn’t actually a person named Rabota furiously cranking out mass quantities of malicious Office files. As it turns out, “Rabota” is the Russian word for work, or job.

While the expected “Admin,” “Test,” “Tester” and “USER” also appeared on the list of malicious Office file authors, there was one entry on the list that was an actual name: “Brian.” With nearly 10% of 2021’s malicious Office files credited to him, Brian must be a busy guy.



# IoT Malware

## IoT Malware Shows Signs of Stabilizing

IoT malware continued to climb last year: SonicWall Capture Labs threat researchers recorded 60.1 million IoT malware hits in 2021, the highest number ever recorded by SonicWall in a single year.

In March, researchers recorded 6.8 million instances of IoT malware, the highest monthly total recorded all year. This didn't come close to beating the monthly record set in October 2020, which saw 10.8 million hits, but higher monthly totals of IoT malware overall resulted in a 6% year-over-year increase.

While an increase in attacks is never *good* news, it's better than it has been. In 2019 and 2020, IoT malware volume

**Higher monthly totals of IoT malware overall resulted in a 6% year-over-year increase.**

rose 218% and 66% respectively. With no corresponding slowdown in the proliferation of connected devices, this suggests attack volumes may be leveling off.

### Global IoT Malware Volume





## IoT Malware by Region

The 6% global increase represented the confluence of several disparate trends. In North America, attacks rose by a moderate 19%. In Europe, IoT malware trended the other way, with researchers observing a 10% decrease year over year.

Asia bore the brunt of the increase. IoT malware there increased 92% year over year, continuing the upward trend observed in 2020, when IoT malware increased by 18%.

More than a third of the world's IoT attacks occurred in the United States. In 2021, the U.S. saw 21.8 million IoT malware hits, a 6% year-over-year increase.

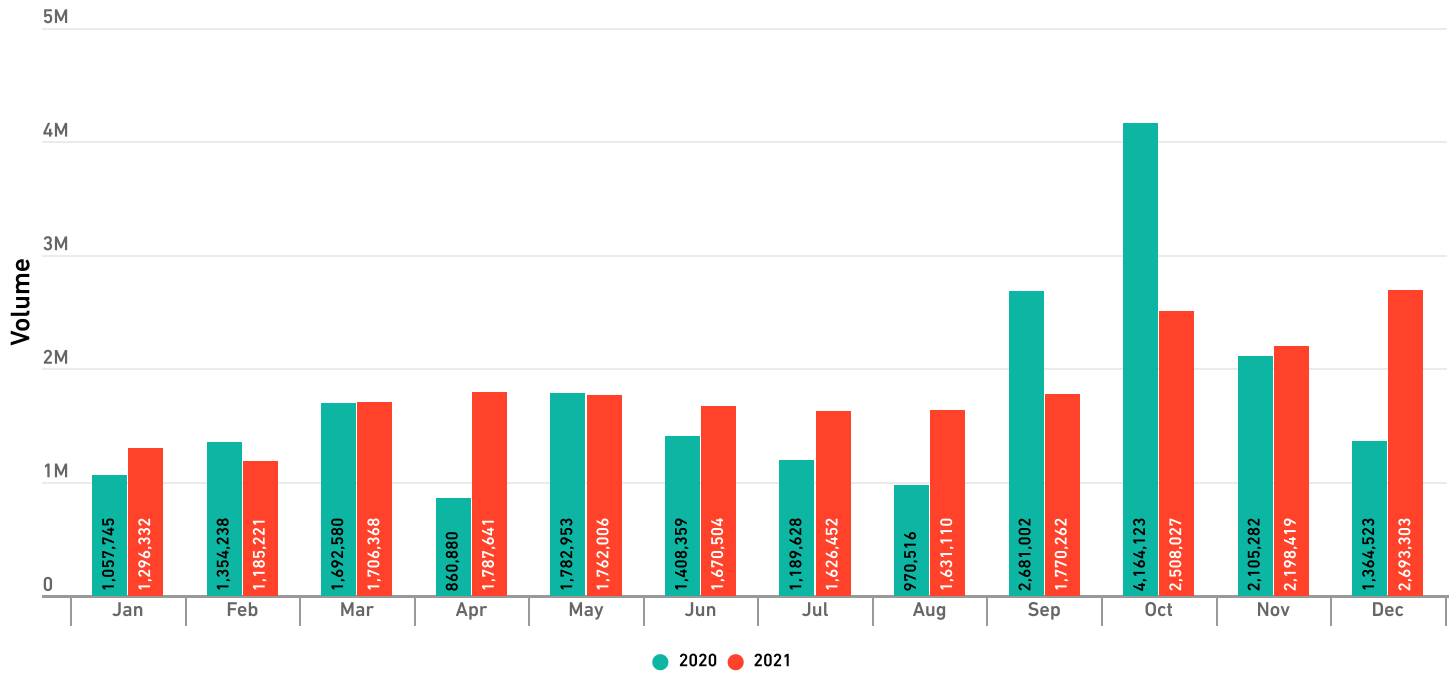
While this mirrors the global increase, the trends in the U.S. looked much different. Globally, IoT malware peaked in Q1, but in the U.S., it didn't peak until Q4. The fact that the

## More than a third of the world's IoT attacks occurred in the United States.

U.S. ended on an upward spike suggests that IoT malware there might make up an even larger percentage of the global total in 2022.

IoT malware volume in the U.K. trended in the opposite direction. IoT malware in the U.K. currently makes up only 3.6% of the global total, but if this trend continues, we expect to see this percentage fall over the next year.

### IoT Malware Volume | United States



# IoT Malware by Industry

SonicWall Capture Labs threat researchers observed increases in IoT malware across all industries studied. The largest jumps were in healthcare, which saw a 71% year-over-year increase, and government, where IoT malware increased 46%. The increase for education and retail was (comparatively) more modest: Both saw IoT malware rise 28%.

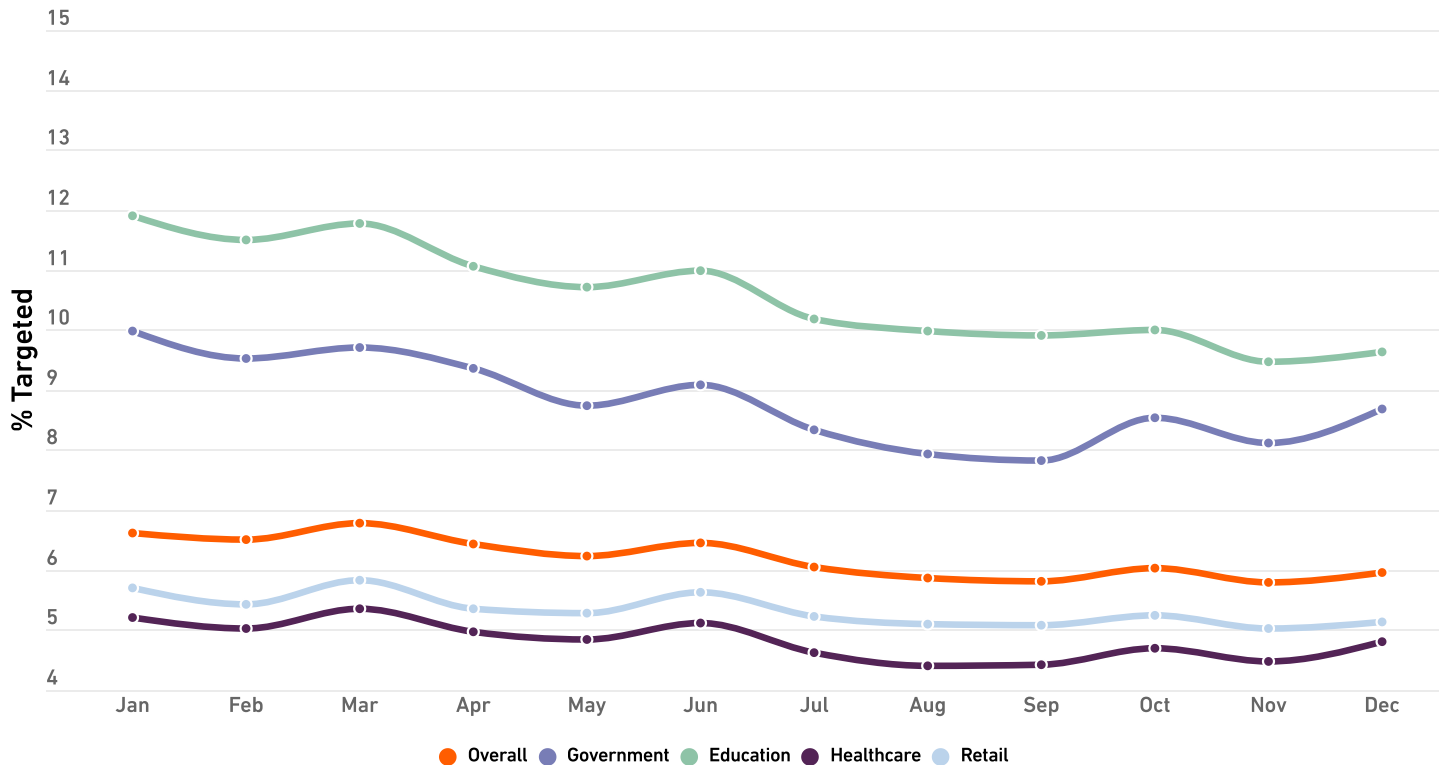
Although education saw one of the smallest decreases, that probably wasn't much comfort to the average 10.5% of education customers targeted each month. But there was one upside: while each industry saw the percentage of customers targeted decrease throughout the year, education saw the biggest drop.

One interesting thing to note: For most attack types, the industry with the lowest percentage of customers targeted is retail. But for IoT malware, it's healthcare. One reason for this

may be the way IoT devices are networked. Due to the life-and-death nature of many healthcare IoT devices, healthcare facilities tend to keep these devices on their own separate and highly secured network, largely inaccessible by other devices.

**The largest jumps were in healthcare, which saw a 71% year-over-year increase, and government, where IoT malware increased 46%.**

### % of Customers Targeted by IoT Malware in 2021

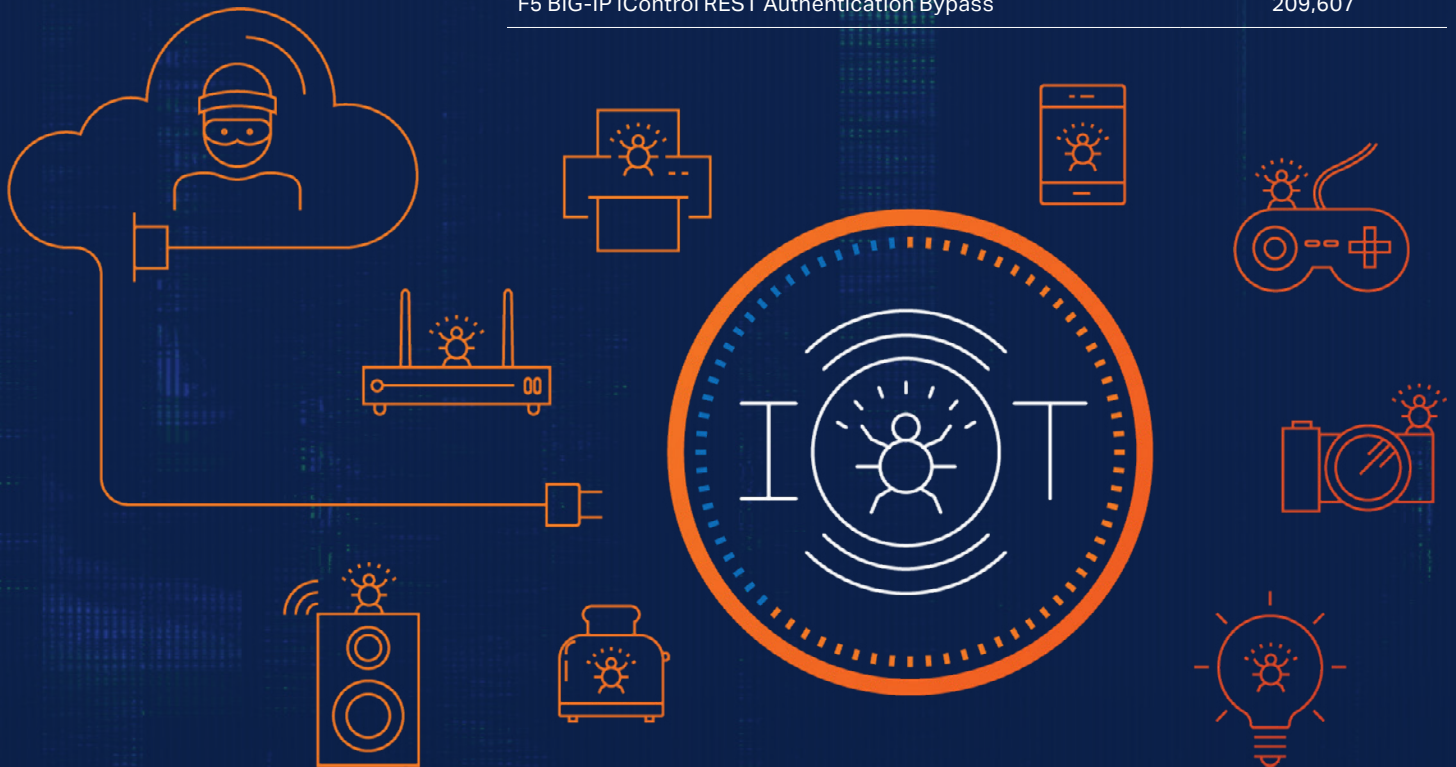


# Protecting the Internet of Things

The number of IoT devices coming onto the market continues to grow. According to IDC, the number of these devices is projected to grow to 55.7 billion by 2025 — together, these devices will produce an estimated 73.1 ZB of data.

Even as new and more powerful IoT devices continue to hit the market, however, the most frequently attacked devices in 2021 were still routers, followed by cameras/NVRs. As of December 2021, SonicWall has 269 signatures protecting more than 96 IoT devices from various threats.

TOP 15 IoT SIGNATURES	HITS
NETGEAR DGN Devices Remote Command Execution 2	26,951,931
D-Link HNAP Request Buffer Overflow	9,655,141
NETGEAR DGN Devices Remote Command Execution	4,768,778
Dasan GPON Routers Command Injection	3,075,947
Vacron NVR Remote Command Execution	2,134,425
D-Link DIR-806 Devices Command Injection	1,663,073
ZyXEL Products Command Execution	1,012,884
Hikvision IP Cameras Authentication Bypass	693,319
Hikvision IP Camera Command Injection	478,233
D-Link DNS-320 system_mgr.cgi Command Injection	440,917
D-Link Products Remote Code Execution	319,804
D-Link DIR-806 Devices Command Injection Vulnerability	277,084
F5 BIG-IP iControl REST Remote Command Execution 2	275,016
D-Link DIR-645 Authentication Bypass	273,605
F5 BIG-IP iControl REST Authentication Bypass	209,607



## Safeguarding by Statute

As IoT malware attack volume continues to rise, governments around the world got serious about ensuring the safety of these devices in 2021.

### The European Union

Introduced in October, [an amendment](#) to the EU's 2014 Radio Equipment Directive would ensure that all wireless devices are sufficiently safe before being sold, require manufacturers to follow new cybersecurity safeguards when designing and producing products, and mandate increased protection for personal data.

### Australia

Due to a lack of response from manufacturers of lower-cost goods, the Australian government announced it is considering making mandatory a suite of voluntary regulations introduced in September 2020. These regulations would outline a set of minimum cybersecurity requirements for consumer-grade smart devices. The Australian government accepted submissions on the specifics of these requirements through Aug. 27 and the crafting of this legislation is ongoing.

### U.S.

In late March, legislation known as the [Cyber Shield Act](#) was reintroduced in Congress. If passed, the law would create security standards for IoT devices based on recommendations from an advisory committee made up of cybersecurity experts from the government, academia and the private sector. Devices meeting these regulations would be allowed to label their products with a mark indicating they had met the standards and their products were more secure.

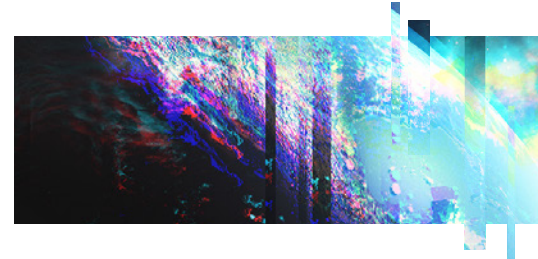
### U.K.

In November, the U.K. Department for Digital, Culture, Media and Sport announced the [Product Security and Telecommunications Infrastructure](#) (PSTI) Bill. This legislation bans universal default passwords, requires manufacturers to disclose the length of time they planned to continue offering security updates for these devices, create a public point of contact for reporting vulnerabilities, and requires devices have the ability to receive software updates.





# Attacks on Non-Standard Ports



## Non-Standard Port Attacks Fall 10%

Some attack types, such as IoT attacks, seem to rise reliably each year. Others, such as malware, trend capriciously, sometimes increasing for years at a time, then falling for the next several months or years before reversing course once again.

Non-standard port attacks follow neither of these patterns.

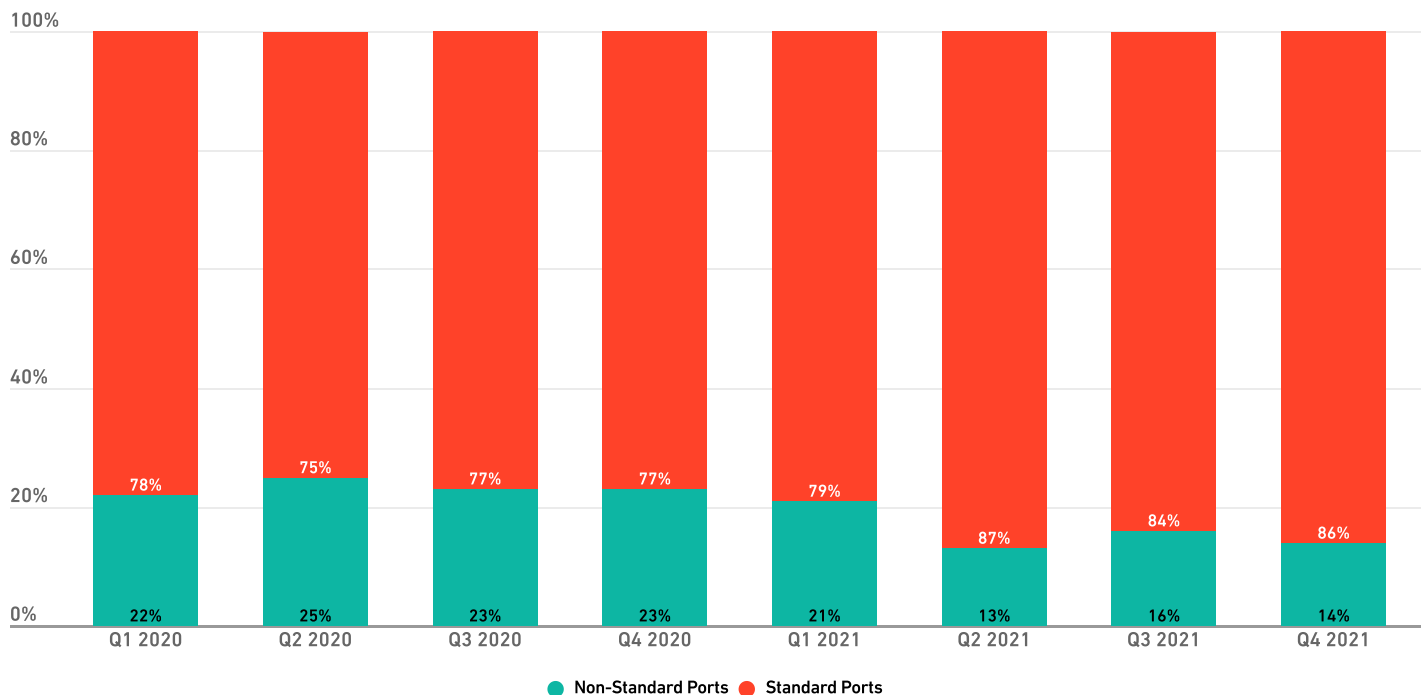
Since SonicWall began tracking non-standard port attacks in 2018, they've followed a consistent, pendulum-like pattern, rising in even-numbered years, and falling in odd.

In 2021, the pendulum swung back, bringing with it a 10% decrease in non-standard port attacks and wiping out most — but not all — of the gain that occurred between 2019 and 2020.

In April, 2021's low-water mark, the percentage of non-standard port attacks fell to 9%, the lowest since January 2019. However, we may not see another month in which these attacks sink below 10%. While the cadence of non-standard port attacks follows a predictable rise-and-fall pattern, we've seen both the crests and the troughs of these attacks trend higher over time.

If this continues to hold true, there's a good chance the 2023 SonicWall Cyber Threat Report will feature non-standard port attacks breaking the 30% mark.

## 2020-21 Global Malware Attacks



## What is a Non-Standard Port Attack?

In networking, a port helps complete the destination or origination network address of a message. About 40,000 ports are registered; however, only a small number — the “standard” ports — are typically used. For example, HTTP uses port 80, HTTPS uses port 443 and SMTP uses port 25. Services using a port that isn’t the one assigned to them by default, usually as defined by the IANA port numbers registry, are using a non-standard port.

There’s nothing inherently wrong with using non-standard ports. But traditional proxy-based firewalls typically focus their protection on traffic passing through the standard ports.

With so many ports to monitor, these legacy firewalls can’t mitigate attacks over non-standard ports. Cybercriminals know this, and target

**With so many ports to monitor, these legacy firewalls can’t mitigate attacks over non-standard ports.**

non-standard ports to increase the odds their payloads can be deployed undetected.

Modern firewalls that are capable of analyzing specific artifacts (as opposed to all traffic) can detect these attacks, making this an increasingly important criteria to look for in a security solution as non-standard ports trend (ever zig-zaggedly) upward.



# Conclusion

## Proactive Defense is the Future of Cybersecurity

Cybercrime has evolved, making it harder for defenders to protect against, detect and stop attacks from entering their networks. As the pace of attacks continues to increase, and the ways attackers breach and infiltrate systems continue to become more targeted and evasive, the future will increasingly belong to the proactive.

Proactive organizations have a thorough understanding of both their network and the threat landscape, allowing them to adapt and shift just as agilely as cybercriminals. This enables them to quickly detect and stop attacks.



### Dark Reading, in partnership with SonicWall,

offers an in-depth discussion on how you can ensure business continuity, protect your employees and customers, and help you maintain compliance with a proactive cybersecurity strategy.

This webinar covers the importance of:

- Having a complete picture of where data lives and how it moves
- Knowing what third parties may be storing data, including cloud vendors, and how they approach security, including their incident response plan
- Employing threat hunting to detect threats that evade existing security controls
- Deploying endpoint protection to look for indicators of compromise and protect the system when potential threats are identified
- Patching vulnerabilities
- And more

[WATCH THE WEBINAR](#)



# About the SonicWall Capture Labs Threat Network



Intelligence for the 2022 SonicWall Cyber Threat Report was sourced from real-world data gathered by the SonicWall Capture Threat Network, which securely monitors and collects information from global devices including:

- More than 1.1 million security sensors in over 215 countries and territories
- Cross-vector, threat related information shared among SonicWall security systems, including firewalls, email security devices, endpoint security solutions, honeypots, content filtering systems and the SonicWall Capture Advanced Threat Protection (ATP) multi-engine sandbox
- SonicWall internal malware analysis automation framework
- Malware and IP reputation data from tens of thousands of firewalls and email security devices around the globe
- Shared threat intelligence from more than 50 industry collaboration groups and research organizations
- Analysis from freelance security researchers

1.1m+

Global Sensors

215+

Countries & Territories

24x7x365

Monitoring

<24hrs

Threat Response

140k+

Malware Samples Collected Daily

28m+

Malware Attacks Blocked Daily





SonicWall Inc.  
1033 McCarthy Boulevard  
Milpitas, CA 95035

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

© 2022 SonicWall Inc.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/ OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION)

ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.

The materials and information contained in this document, including, but not limited to, the text, graphics, photographs, artwork, icons, images, logos, downloads, data and compilations, belong to SonicWall or the original creator and is protected by applicable law, including, but not limited to, United States and international copyright law and regulations.

## About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit [www.sonicwall.com](http://www.sonicwall.com) or follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).



SonicWall, Inc.  
1033 McCarthy Boulevard | Milpitas, CA 95035

SONICWALL\*

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.